MANGELNDE NORMENKLARHEIT IM DATENSCHUTZ-STRAFRECHT

Eine empirische Untersuchung der Datenschutz-Kriminalität mit reformpolitischen Schlußfolgerungen und Vorschlägen

INAUGURAL-DISSERTATION

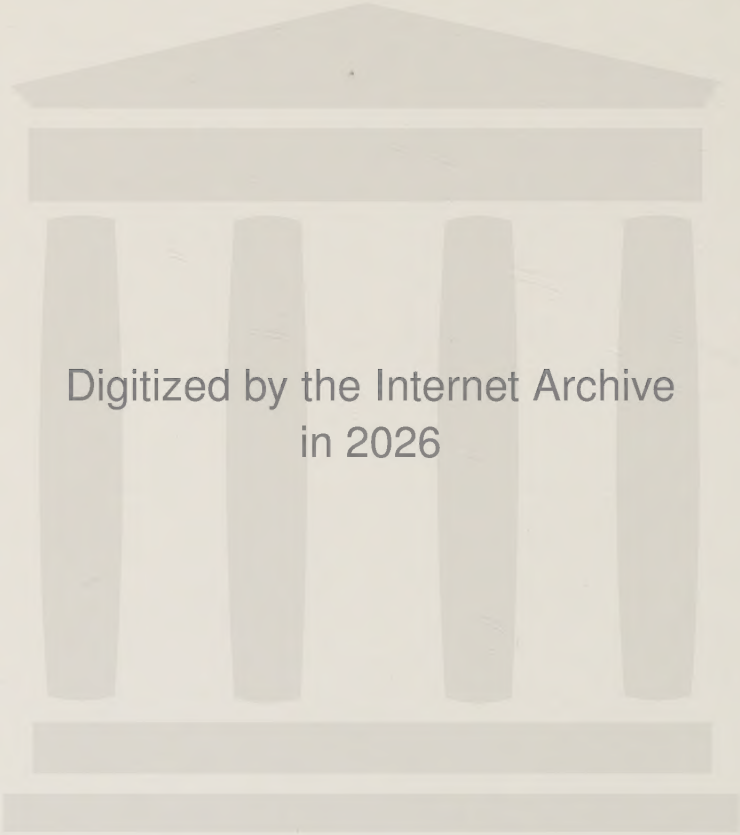
zur Erlangung der Doktorwürde der
Juristischen Fakultät
der Eberhard-Karls-Universität zu Tübingen

vorgelegt von
Armin Herb
aus Göppingen

1984

85 2

Univ. Leiden Bibl.


Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41536517_0005

MANGELNDE NORMENKLARHEIT IM DATENSCHUTZ-STRAFRECHT

Eine empirische Untersuchung der Datenschutz-Kriminalität mit reformpolitischen Schlußfolgerungen und Vorschlägen

INAUGURAL-DISSERTATION

zur Erlangung der Doktorwürde der
Juristischen Fakultät
der Eberhard-Karls-Universität zu Tübingen

vorgelegt von
Armin Herb
aus Göppingen

1984

Dekan:	Prof. Dr. Günter Püttner
1. Berichterstatter:	Prof. Dr. Fritjof Haft
2. Berichterstatter:	Prof. Dr. Jürgen Baumann

Tag der mündlichen Prüfung: 18. Dezember 1984

Inhaltsverzeichnis

Abkürzungen IV
Verzeichnis der Abbildungen und Tabellen VIII
Fälleverzeichnis IX
Literaturverzeichnis XI

§ 1 Einleitung (einschließlich Gang der Untersuchung)..... 1

§ 2 Die Datenschutzgesetzgebung..... 7

A) Die Entwicklung in der Bundesrepublik Deutschland 7

I) Der parlamentarische Beginn 7
II) Die ersten Gesetzesentwürfe auf Bundesebene 8
III) Die Lage in den Bundesländern 12
IV) Die Entwicklung nach Verabschiedung des BDSG 14

B) Die Entwicklung im Ausland 16

I) Frankreich 16
II) Schweiz 18
III) Österreich 19
IV) Schweden 21
V) Vereinigte Staaten von Amerika 22
VI) Großbritannien 24

§ 3 Die Verweisungstechnik der Datenschutzgesetze 25

A) Die Verweisungstechnik 27

I) Die Klassifizierung von Verweisungen 27
II) Die Problematik von Verweisungen 30
III) Die psycho-biologische Verständnisgrenze 33

B) Die Verweisungen des BDSG 39

I) Die Darstellung der strukturellen Komplexität anhand eines "Verweisungsbaumes" 39
II) Das Ergebnis der Strukturdarstellung 41
III) Die Darstellung der quantitativen Komplexität anhand der sprachl. Auflösung der Definationen ... 46
IV) Das Ergebnis der sprachlichen Auflösung 51

C) Exkurs: Die Strafbestimmungen des Sozialgesetzbuches und die Darstellung ihrer Verweisungskomplexität..... 54

§ 4 Grundlagen und Methodik der empirischen Auswertung einschl. deren Verfahrenscharakteristika 57

A) Grundlagen der Auswertung 57

I) Erlangung der Akten und Einsichtnahme 58
II) Abgrenzung des Untersuchungszeitraumes 62

B) Methodik der Auswertung 63

I) Wahl der Untersuchungsmethode 63
II) Gang der Konstruktion des Auswertungsbogens 64
III) Arten der Auswertungskriterien 66
IV) Bildung der Kriterien des Auswertungsbogens 67
V) Durchführung der Erhebung, statistische Auswertung und Darstellung der Ergebnisse 68

C) Verfahrenscharakteristika 69

I) Anzeigenerstatter 69
II) Stelle der Anzeigeneinleitung 70
III) Grund der Anzeige 72
IV) Verfahrensbeendigung 74
V) Verfahrensdauer 78
VI) Umfang und Bedeutung von Sachverständigen 79

§ 5 Auswertung zum Problem des Schutzbereiches der Datenschutzgesetze 81

A) Das Kriterium "Datei" als Anwendungsvoraussetzung 81

I) Die Auslegung des Begriffs "Datei" 82
II) Auswertung nach Speicherort ("Quelle") der Daten ... 86
III) Gruppe "Nicht-Datei" 89
IV) Gruppe "EDV-Anlagen" 90
V) Gruppe "Graubereich" 97

B) Ausgrenzungen vom Anwendungsbereich 116

I) Interne Daten 116
II) Medienprivileg 121

§ 6 Die personenbezogenen und die offenkundigen Daten in der Auswertung 129

A) Personenbezogene Daten 129

B) Offenkundige Daten 132

I) Auswertungsergebnisse 132
II) Die Auslegung des Begriffs "offenkundig" 133

§ 7 Auswertung zum Problem der Tatmodalitäten 147

A) Die faktische Relevanz der einzelnen Tatmodalitäten 148

B) Interpretation und Analyse der einzelnen Tatmodalitäten . 151

I) Abrufen 151
II) Sich verschaffen 157
III) Übermitteln 160
IV) Verändern 164
V) Speichern 165
VI) Löschen 166

§ 8 Auswertung zur Strafantragsproblematik 169

A) Die Problemstellung 169

B) Die Auswertung der tatsächlichen Antragsteller 171

I) Strafanträge von Landesdatenschutzbeauftragten 172
II) Strafanträge von Betroffenen 172

C) Strafantragsrecht der "speichernden Stelle"? 175

I) Ergebnisse der Auswertung 175
II) Auslegung des Strafantragsrechts 177

D) Öffentliches Interesse bei § 21 III NDSG 180

§ 9 Zusammenfassende Würdigung und Reformvorschläge 183

A) Zusammenfassende Würdigung 183

I) Tatsächliches Ausmaß der Delikte und Dunkelziffer .. 185
II) Gründe für eine hohe Dunkelziffer 187
III) Zukünftige Entwicklung 189
IV) Schlußfolgerungen 190
V) Die Datenschutzprinzipien "Einwilligung" und "Zweckbindung" 194
VI) Das "Quantitätskriterium" als tragendes Prinzip 197
VII) Konsequenzen des Quantitätskriteriums 200

B) Datenschutzrechtliche Reformvorschläge 202

I) Allgemeine Reformüberlegungen 203
II) Strafrechtliche Reformüberlegungen 204
III) Standort und inhaltliche Erfordernisse einer Strafnorm 207
IV) Reform der Strafverfolgungsvoraussetzungen 212
V) Eigener Vorschlag für eine Strafnorm 219

Anhang: Fälle 225

Auswertungsbogen 265

ABKÜRZUNGEN

a. A.	andere(r) Ansicht
a. a. O.	am angegebenen Ort
Abb.	Abbildung
Abs.	Absatz
ADV	Automatisierte Datenverarbeitung
a. F.	alte Fassung
AfP	Archiv für Presserecht (Zeitschrift)
AG	Amtsgericht
allg.	allgemein(e/er/es)
Anh.	Anhang
Anl.	Anlage(n)
Anm.	Anmerkung(en)
AöR	Archiv des öffentlichen Rechts
ARSt	Arbeitsrecht in Stichworten. Arbeitsrechtliche Entscheidungssammlung
Art.	Artikel
AT	Allgemeiner Teil
Aufl.	Auflage
AusfG	Ausführungsgesetz
BAnz	Bundesanzeiger
BayVerfGH	Bayerischer Verfassungsgerichtshof
BayVGH	Bayerischer Verwaltungsgerichtshof
BayDSG	Bayerisches Gesetz zum Schutz vor Mißbrauch personenbezogender Daten bei der Datenverarbeitung (Bayerisches Datenschutzgesetz)
BB	Betriebs-Berater (Zeitschrift)
Bd.	Band (Bände)
BDSG	Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz)
Begr.	Begründung
Bem.	Bemerkung(en)
BfD	Bundesbeauftragter für den Datenschutz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen
BKA	Bundeskriminalamt
BKAG	Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes (Bundeskriminalamtes)
BKK	Die Betriebskrankenkasse (Zeitschrift)
BlnDSG	Gesetz über den Datenschutz in der Berliner Verwaltung (Berliner Datenschutzgesetz)
BR-Drs.	Drucksache des Bundesrates
BrDSG	Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bremisches Datenschutzgesetz)
BT	Besonderer Teil
BT-Drs.	Drucksachen des Deutschen Bundestages
Btx	Bildschirmtext

BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
BVwVfG	Bundesverwaltungsverfahrensgesetz
BW	Baden-Württemberg
BWV	Bundeswehrverwaltung (Zeitschrift)
BWVPr	Baden-Württembergische Verwaltungspraxis (Zeitschrift)
bzgl.	bezüglich
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz)
DANA	Datenschutz-Nachrichten (Zeitschrift)
DaSta	Datenstation
DB	Der Betrieb (Zeitschrift)
ders.	derselbe
Die Polizei ...	gleichnamige Zeitschrift
Diss.	Dissertation
DJT	Deutscher Juristentag
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
Dok.	Dokument(ation)
DOK	Die Ortskrankenkasse (Zeitschrift)
DRiZ	Deutsche Richterzeitung
DRV	Deutsche Rentenversicherung (Zeitschrift)
DSWR	Datenverarbeitung, Steuer, Wirtschaft, Recht (Zeitschrift)
DuD	Datenschutz und Datensicherung (Zeitschrift)
DuR	Demokratie und Recht (Zeitschrift)
DV	Datenverarbeitung
DVBl	Deutsches Verwaltungsblatt (Zeitschrift)
DVD	Deutsche Vereinigung für Datenschutz
DVR	Datenverarbeitung im Recht (Zeitschrift)
EDV	Elektronische Datenverarbeitung
EGStGB	Einführungsgesetz zum Strafgesetzbuch
Einf.	Einführung
Einl.	Einleitung
Erl.	Erläuterung(en) bzw. Erlaß
EWR	Schriftenreihe zum Europäischen Weinrecht
f.	folgende
FernmG	Fernmeldeanlagengesetz
ff.	fortfolgende
FN	Fußnote(n)
FS	Festschrift
FuR	Film und Recht (Zeitschrift)
G	Gesetz
GA	Goltdammer's Archiv für Strafrecht
GABl.	Gemeinsames Amtsblatt des (jeweiligen) Landes
GBl.	Gesetzblatt
GDD	Gesellschaft für Datenschutz und Datensicherung
GewArch	Gewerbearchiv (Zeitschrift)
GG	Grundgesetz für die Bundesrepublik Deutschland
ggf.	gegebenenfalls
GMBl.	Gemeinsames Ministerialblatt
GMD	Gesellschaft für Mathematik und Datenverarbeitung

GrKG	Grundlagenstudium aus Kybernetik und Geisteswissenschaften
GVBl.	Gesetz und Verordnungsblatt
HDSG	Hessisches Datenschutzgesetz
h. L.	herrschende Lehre
h. M.	herrschende Meinung
HmbDSG	Hamburgisches Datenschutzgesetz
Hrsg.	Herausgeber
i. d. F.	in der Fassung
i. d. R.	in der Regel
INPOL	Elektronisches Informations- und Auskunftssystem der Polizei
i. S.	im Sinne
JA.	Juristische Arbeitsblätter (Zeitschrift)
JR.	Juristische Rundschau (Zeitschrift)
JURA	Juristische Ausbildung (Zeitschrift)
JURIS	Juristisches Informationssystem des Bundesministeriums der Justiz
JuS	Juristische Schulung (Zeitschrift)
JVA	Justizvollzugsanstalt
JZ	Juristenzeitung
Kap.	Kapitel
Kfz	Kraftfahrzeug
KG	Kammergericht
Komm.	Kommentar, Kommentierung
KpS	Kriminalpolizeiliche (personenbezogene) Sammlung(en)
Kriminalistik .	gleichnamige Zeitschrift
KSchG	Kündigungsschutzgesetz
LAG	Landesarbeitsgericht
LDatG RP	Landesgesetz zum Schutze des Bürgers bei der Verarbeitung personenbezogener Daten (Landesdatenschutzgesetz des Landes Rheinland-Pfalz)
LDSG BW	Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Landesdatenschutzgesetz) des Landes Baden-Württemberg
LDSG NW	Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Datenschutzgesetz Nordrhein-Westfalen)
LDSG SH	Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Landesdatenschutzgesetz Schleswig-Holstein)
LfD	Landesbeauftragter für Datenschutz
LG	Landgericht
Lit.	Literatur
LKA	Landeskriminalamt
LT-Drs.	Drucksachen des (jeweiligen) Landtags
m. Anm.	Mit Anmerkung(en)
MDR	Monatsschrift für Deutsches Recht (Zeitschrift)
Mistra	Anordnung über Mitteilung in Strafsachen (bundeseinheitliche Regelung)
MRRG	Melderechtsrahmengesetz
mwN	mit weiteren Nachweisen

NDSG	Niedersächsisches Datenschutzgesetz
n. F.	neue Fassung bzw. neue Folge
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NStZ	Neue Zeitschrift für Strafrecht
ÖVD	Öffentliche Verwaltung und Datenverarbeitung (Zeitschrift)
OLG	Oberlandgericht
OVG	Oberverwaltungsgericht
OVGE	Entscheidungen der Oberverwaltungsgerichte
OWiG	Gesetz über Ordnungswidrigkeiten
RA	Rechtsanwalt
RegEntw	Regierungsentwurf
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren
RIW/AWD	Recht der internationalen Wirtschaft/Außenwirtschaftsdienst des Betriebs-Berater (Zeitschrift)
RN	Randnummer(n)
Rspr.	Rechtsprechung
RuP	Recht und Politik (Zeitschrift)
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SDSG	Saarländisches Datenschutzgesetz
sec.	Sekunde
SGB X	Sozialgesetzbuch Zehntes Buch - Verwaltungsverfahren -
StA	Staatsanwaltschaft bzw. Staatsanwalt
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
Tab.	Tabelle
TB	Tätigkeitsbericht
VBlBW	Verwaltungsblätter für Baden-Württemberg
VersR	Versicherungsrecht (Zeitschrift)
VerwArch	Verwaltungsarchiv
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
VOP	Verwaltungsführung, Organisation, Personalwesen (Zeitschrift)
VW	Versicherungswirtschaft (Zeitschrift)
VwVfG	Verwaltungsverfahrensgesetz
wistra	Zeitschrift für Wirtschaft, Steuer, Strafrecht
ZEVIS	Zentrales Verkehrsinformationssystem beim Kraftfahrtbundesamt
ZPO	Zivilprozeßordnung
ZRP	Zeitschrift für Rechtspolitik
ZSR	Zeitschrift für schweizerisches Recht

Verzeichnis der Abbildungen und Tabellen

A) Abbildungen:

Abb. 3.1	"Informationsverarbeitung"	§ 3 A III 1	33
Abb. 3.2	"Komplexitätsfolgen"	§ 3 A III 2	39
Abb. 3.3	"Verweisungsbaum"	§ 3 B I	40
Abb. 3.4	"Definitionsauflösung"	§ 3 B III	49
Abb. 3.5	"Sozialdaten-Schutz"	§ 3 C	56
Abb. 6.1	"Struktur 'Offenkundigkeit'"	§ 6 B II	134
Abb. 7.1	"Datenabruf"	§ 7 B I 3	155
Abb. 7.2	"Datenweitergabe"	§ 7 B III 1	161
Abb. 9.1	"§ 41 BDSG-Strafbarkeit"	§ 9 A IV	193

B) Tabellen:

Tab. 4.1	"BKA-Statistik"	§ 4 A	58
Tab. 4.2	"Anzeigenerstatter"	§ 4 C II	71
Tab. 4.3	"Stelle der Anzeigeneinleitung"	§ 4 C II	72
Tab. 4.4	"Begleitdelikte"	§ 4 C III	73
Tab. 4.5	"Verfahrensbeendigung"	§ 4 C IV	75
Tab. 4.6	"Einstellungsbegründungen"	§ 4 C IV 2	77
Tab. 4.7	"Verfahrensdauer"	§ 4 C V	78
Tab. 5.1	"Speicherort ("Quelle")"	§ 5 A II	87
Tab. 5.2	"Speicherortbereiche"	§ 5 A II	88
Tab. 5.3	"EDV-Anlagen-Verteilung"	§ 5 A IV	91
Tab. 5.4	"StA und EDV-Anlagen"	§ 5 A IV	93
Tab. 5.5	"Graubereich"	§ 5 A V	97
Tab. 7.1	"Handlungsvarianten"	§ 7 A	150
Tab. 8.1	"Strafantragsteller"	§ 8 B	171
Tab. 8.2	"Strafantragsmöglichkeiten LfD"	§ 8 B I	172

FÄLLEVERZEICHNIS

Angegeben ist der Fundort der ausführlich(st)en Falldarstellung:

Fall 1	("Universitätsoperator")	§ 3 B IV	52
Fall 2	("Steuerunterlagen")	§ 4 A I	60
Fall 3	("Einkommenshöhe")	Anhang	225
Fall 4	("Taxifahrer")	Anhang	225
Fall 5	("Vorstandsvorsitzender")	Anhang	226
Fall 6	("Abschiedsabruf")	§ 5 A IV	94
Fall 7	("Motorradzulassung")	§ 6 A	131
Fall 8	("Verkehrsunfall")	Anhang	228
Fall 9	("Zusammenarbeit")	§ 5 A IV	95
Fall 10	("Jugendstrafe")	Anhang	228
Fall 11	("Versicherungsverlauf")	§ 5 A IV	96
Fall 12	("Hellseherin")	Anhang	229
Fall 13	("Betriebsrat")	Anhang	231
Fall 14	("Häftlingsadresse")	§ 5 A V 1 b) bb)	105
Fall 15	("Nachbarsjunge")	Anhang	232
Fall 16	("Drittschuldnerliste")	§ 5 A V 2) a)	107
Fall 17	("Aktienhandel")	§ 5 A V 2) a)	107
Fall 18	("Werbeliste")	§ 5 A V 2) b)	107
Fall 19	("Roulettspieler")	Anhang	233
Fall 20	("Bibliotheksbenutzerausweis")	Anhang	234
Fall 21	("Mikrofichesfund")	Anhang	235
Fall 22	("Spenderlisten")	§ 5 A V 3) b)	111
Fall 23	("Kreditangebote")	Anhang	237
Fall 24	("Mitgliederabwerbung")	Anhang	237
Fall 25	("Mikroficheeinsicht")	Anhang	238
Fall 26	("Zeitungsabonnenten")	Anhang	239
Fall 27	("Multifunktionär")	Anhang	240
Fall 28	("Geburtsdatum")	§ 5 B II	125
Fall 29	("Aprilscherz")	§ 5 B II	126
Fall 30	("Einkaufsgenossenschaft")	§ 5 B II	126
Fall 31	("Getrenntleben")	§ 6 A	130
Fall 32	("Bankindiskretion")	Anhang	240
Fall 33	("Reklamesendung")	§ 6 B II 1)	141
Fall 34	("Studienfachangabe")	Anhang	241
Fall 35	("Viehstatistik")	Anhang	242
Fall 36	("informatorische Anfrage")	Anhang	243

Fall 37	("Bankauskunft")	Anhang	243
Fall 38	("Karteikastenraub")	Anhang	244
Fall 39	("Telefondatenerfassung")	Anhang	245
Fall 40	("Zentralnamenskartei")	Anhang	245
Fall 41	("Tischcomputer")	§ 7 B VI	167
Fall 42	("HEPOLIS-Abruf")	§ 8 B II	173
Fall 43	("Studentenkartei")	§ 8 B II	173
Fall 44	("Interessenverein")	§ 8 B II	174
Fall 45	("Löschungsbegehren")	Anhang	246
Fall 46	("Meisteranerkennung")	Anhang	247
Fall 47	("Buchclub")	Anhang	248
Fall 48	("Jungwählerin")	Anhang	248
Fall 49	("Flurbereinigung")	Anhang	249
Fall 50	("Nötigungsversuch")	Anhang	249
Fall 51	("Nebenberuf")	Anhang	250
Fall 52	("Lebenslauf")	Anhang	251
Fall 53	("Polizeiausdrucke")	Anhang	251
Fall 54	("Schuldnerkartei")	Anhang	252
Fall 55	("Krankheitsdaten")	Anhang	252
Fall 56	("Geschäftsfreundin")	Anhang	253
Fall 57	("Verlobtenfinanzen")	Anhang	254
Fall 58	("Baukasse")	Anhang	254
Fall 59	("Nachbarstreitigkeiten")	Anhang	255
Fall 60	("Erbschaftsstreit")	Anhang	258
Fall 61	("Doppelhaushälfte")	Anhang	258
Fall 62	("Kontaktaufnahme")	Anhang	258
Fall 63	("Restrisiko")	Anhang	259
Fall 64	("Ehevermittler")	Anhang	260
Fall 65	("Unterstützungsunterschriften")	Anhang	261
Fall 66	("Versicherungskarteikarten")	Anhang	261
Fall 67	("Programmdopplung")	Anhang	262
Fall 68	("Handwerkersorgen")	Anhang	263
Fall 69	("Scheidungsfolgen")	Anhang	263
Fall 100	("Nachnahmelieferung")	§ 6 B II 3)	144
Fall StA	Berlin	Anhang	264

LITERATURVERZEICHNIS

ABEL, Ralf Bernd; PETERS, Hans
- Hamburgisches Datenschutzgesetz (HmbDSG) Textausgabe und Kommentar des HmbDSG, Hrsg.: Gesellschaft für Datenschutz und Datensicherung (GDD-Handtexte), Köln 1982 (zitiert: Abel/Peters)

ALKE, Horst H.
- Datenschutz - Schutz vor Neuen Medien? in: DuD 1982 S. 86 - 93

ARZT, Gunther; WEBER, Ulrich
- Strafrecht BT, LH 1: Delikte gegen die Person, 2. Aufl. Bielefeld 1981 (zitiert: Arzt/Weber)

ARZT, Gunther
- Die Ahndung von Verstößen gegen den Datenschutz in: Aktuelle Beiträge über den Datenschutz, Schriftreihe Schimmelpfeng, Bd. 9, Frankfurt/M. 1977, S. 127 - 136

AUERBACH, Heinz
- Die eigenhändigen Delikte unter besonderer Berücksichtigung der Sexualdelikte des 4. StrRG (Europ. Hochschulschriften. Reihe 2. Bd. 200) Frankfurt/M. 1978

AUERNHAMMER, Herbert
- Bundesdatenschutzgesetz, Kommentar, 2. Aufl. Köln 1981; (zitiert: Auernhammer, Kommentar)

BADEN, Eberhard
- Dynamische Verweisungen und Verweisungen auf Nichtnormen in: NJW 1979 S. 623 - 627

BARTL, Harald
- Handbuch Btx-Recht mit einem Kommentar zum Bildschirmtext-Staatsvertrag, Heidelberg 1984

BAUKNECHT, Kurt
- Computer-Kriminalität S. 99 - 112 in: Wirtschaftskriminalität. Wissenschaftliche Beiträge zum 50jährigen Bestehen der Neutra Treuhand AG, Selbstverlag Neutra Treuhand AG, Zürich 1982

BAUMANN, Jürgen
- Die natürliche Wortbedeutung als Auslegungsgrenze im Strafrecht in: MDR 1958 S. 394 - 396

- Strafrecht. Allgemeiner Teil. 8. Aufl. Bielefeld 1977 (zitiert: Baumann AT)

BAUMANN, Jürgen; DÄHN, Gerd - Studien zum Wirtschaftsstrafrecht (Juristische Studien, 36.), Tübingen 1972 (zitiert: Baumann/Dähn)

BAUTSCH, Joachim - Datenschutzrecht in Niedersachsen, Rechts- und Verwaltungsvorschriften mit Erläuterungen Köln 1978

BECKER, Hans Joachim - Grundprobleme des Datenschutzes in: Schleswig-Holsteinische Anzeigen 1980 S. 25 - 33

BENDA, Ernst - Privatsphäre und "Persönlichkeitsprofil" S. 23 - 44 in: Festschrift für Willi Geiger (1974), (zitiert: Benda, FS Geiger)

BERCKHAUER, Friedrich-Wilhelm - Die Strafverfolgung bei schweren Wirtschaftsdelikten: Bericht über eine Aktenuntersuchung (Kriminologische Forschungsbereichte aus dem Max-Planck-Institut für Ausländisches und Internationales Strafrecht, Freiburg, Bd. 4) Freiburg 1981

BERG, Wilfried - Das Bundesdatenschutzgesetz - Ein Überblick in: JA 1983 S. 245 - 249

BERGER, Albrecht - Die Erschließung von Verweisungen bei der Gesetzesdokumentation, Bd. 3 der "Informations-Systeme - Grundlagen und Praxis der Informationswissenschaften", München-Pullach 1971

BERGMANN, Lutz; MÖHRLE, Roland - Datenschutzrecht - Handkommentar zum BDSG Teil III, Kommentar, Loseblatt, 3. Erg. Liefg. (Stand: Mai 1982), Stuttgart 1977 (zitiert: Bergmann/Möhrle)

BERNHARD, U.; GOLA, P.; TUNER, L. - Übersetzung des französischen Datenschutzgesetzes, DuD 3/1978, S. 157 - 162

BERZ, Ulrich - Die Dokumentationsbeiträge der Strafrechtslehrertagung 1977 in Giessen, Tagungsbericht in: ZStW 90 (1978) S. 210 - 234

BLESGEN, Gregor; WEIHE, Hermann Joachim - Kostenmäßige Auswirkungen des Bundesdatenschutgesetzes für die Wirtschaft in: DB 1977 S. 433 - 438

BRINCKMANN, Hans - Juristische Fachsprache und Umgangssprache in: ÖVD 1972 S. 60 - 69

BRÖDNER, Peter;
KRÜGER, Detlef;
SENF, Bernd
- Der programmierte Kopf - Eine Sozialgeschichte der Datenverarbeitung, Berlin 1981 (zitiert: Brödner)

BULL, Hans Peter
- Medienprivileg - offene Flanke des Datenschutzes?
in: FuR 8/1979 S. 395 - 402

- Zur verfassungsrechtlichen Verankerung des Datenschutzes
in: ÖVD 11/1979 S. 3 - 9

- Ziele und Mittel des Datenschutzes - Forderungen zur Novellierung des BDSG, Königstein/Ts. 1981 (zitiert: Bull, Ziele)

- Datenschutz und neue Medien - Problemskizze des BfD
in: DuD 1982 S. 147 - 152

- Tätigkeitsberichte des BfD:
1. TB veröffentlicht in: Schriftenreihe "Zur Sache" 2/79, Hrsg. Deutscher Bundestag;
2. TB vom 18.01.1980, BT-Drs. 8/3570;
3. TB vom 09.01.1981, BT-Drs. 9/83;
4. TB vom 30.12.1981, BT-Drs. 9/1243;
5. TB vom 13.01.1983, BT-Drs. 9/2386

BULL, Hans Peter;
ZIMMERMANN, Gerhard
- Herstellung und Vertrieb von Fachzeitschriften als Gegenstand des Datenschutzrechts
in: AfP 3/1978 S. 111 - 115

- Das Medienprivileg - Kriterien der Abgrenzung und inhaltlichen Bestimmung - in: FuR 3/1979 S. 118 - 122

BURHENNE, Wolfgang E.;
PERBAND, Klaus
- EDV-Recht, Systematische Sammlung der Rechtsvorschriften, organisatorische Grundlagen und Entscheidungen zur elektronischen Datenverarbeitung. 3. Band: Kommentar zum BDSG, bearbeitet von R. Kamlah, W. Schimmel und E. Schwan; Loseblatt, 37. Liefg., Stand: Mai 1984, Berlin 1970 (zitiert: Burhenne/Perband)

BURKERT, Herbert
ENGEL, Stefan
- Datenschutz in Europa
in: DuD 1980 S. 146 - 152

COBLER, Sebastian
- DAZUSY, PSI und MOPS - Computer auf den Spuren von "Risikopersonen"
in: Kursbuch 66, 1981 S. 7 - 18

DÄSTNER, Christian
- Kriminalität in der Bundesrepublik - Ausmaß und Reaktion, Göttingen 1972

DAMMANN, Ulrich
- Erste Erfahrungen mit dem BDSG
in: NJW 1978 S. 1906 - 1907

DANZIG, Rainer; JESCHEK, Peter; EGGER, Josef - Der Weg ins Gefängnis. Der Einfluß von familiärer Sozialisation und behördlicher Selektion auf die Entstehung von Straffälligkeit. Eine empirische Untersuchung. Weinheim 1979

DEHM, Walter - Verbesserung des Datenschutzes in: DSWR 1980 S. 183 - 185

DEUBNER, Karl G. - Anmerkungen zu OLG Düsseldorf NJW 1969, 623 in: NJW 1969 S. 623

DÖLLE, Hans - Vom Stil der Rechtssprache in: Recht und Staat, Heft 138/139, Tübingen 1949

DORSCH, Friedrich - Psychologisches Wörterbuch, 9. Aufl., Bern, Stuttgart, Wien 1976

DREHER, Eduard; TRÖNDLE, Herbert - Strafgesetzbuch, Kommentar, 41. Aufl. München 1983

EGLOFF, Willi - Braucht die Schweiz ein Datenschutzgesetz? in ZSR 96 (1977) I S. 345 - 368

EGLOFF, Willi; SCHIMMEL, Wolfgang - Die "Magna Charta des Bürgers von heute"? Anmerkungen zum neuen BDSG in: DuR 1977 S. 124 - 138 (zitiert: Egloff/Schimmel)

ERNESTI, Günter - Informationsverbund Justiz - Polizei in: NJW 1983 S. 57 - 63

FIEDLER, Herbert - Datenschutz und Gesellschaft S. 179 - 195 in: Informationsrecht und Informationspolitik, (Hrsg.: Wilhelm Steinmüller), München 1976 (Rechtstheorie und Informationsrecht, Bd. 1) (zitiert: Fiedler in: Steinmüller, Informationsrecht)

- "Unbestimmte Rechtsbegriffe" in Datenschutzgesetzen in: DuD 1980 S. 75 - 78

- Anmerkungen zu BGH JZ 1984, 676 - 678 (= NJW 1984, 1886) in: JZ 1984 S. 678 - 679

FRANK, Helmar - Kybernetische Grundlagen der Pädagogik, 2. Bd., 2. Aufl. Baden-Baden 1969 (zitiert: Frank, Kybernetische Grundlagen)

- Informationspsychologie in: Kybernetik. Brücke zwischen den Wissenschaften, 3. Aufl. Frankfurt/M. 1964 (zitiert: Frank, Informationspsychologie)

GALLWAS, Hans-Ullrich
- Verfassungsrechtliche Grundlagen des Datenschutzes
in: Der Staat, Zeitschrift für Staatslehre, öffentliches Recht und Verfassungsgeschichte, 18. Band 1979 S. 507 - 520

GALLWAS, Hans Ullrich; SCHEIDER, Jochen; SCHWAPPACH, Jürgen; SCHWEINOCH, Joachim; STEINBRINCK, Tilo
- Datenschutzrecht. Kommentar und Vorschriftensammlung, Loseblatt, Stand D-z 1981 (5. Liefg.) Stuttgart 1978
(zitiert: Gallwas/S/S)

GARSTKA, Hansjürgen
- Mediendatenbanken und Datenschutz
in: JZ 1978 S. 507 - 511

- Anforderungen des Datenschutzes an Gesetze auf dem Gebiet der neuen Medien
in: DuD 1982 S. 153 - 156

GEIGER, Hansjörg
- Das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983
in: DSWR 1984 S. 43 - 46

GEIGER, Hansjörg; SCHNEIDER, Jochen
- Der Umgang mit Computern - Möglichkeiten und Probleme ihres Einsatzes, München 1975
(zitiert: Geiger/Schneider)

GERTH, E.
- Marktwirtschaft und Datenschutz - Auszug aus einem aktuellen Gutachten
in: DuD 1983 S. 9 - 14

GÖPPINGER, Hans
- Kriminologie 4. Aufl. München 1980

GOLA, Peter
- Das BDSG schafft neue Rechte für den Bürger
in: MDR 1977 S. 448 - 453

- Die Datenschutzgesetze der Bundesländer - ein Überblick
in: MDR 1980 S. 181 - 184

- Die Entwicklung des Datenschutzrechts im Jahr 1981
in: NJW 1982 S. 1498 - 1505

- Datenschutz in der Rechtsprechung
in: DSWR 1983 S. 91 - 95

GOLA, Peter; HÜMMERICH, Klaus; KERSTAN, Uwe
- Datenschutzrecht. Erläuterte Rechtsvorschriften und Materialien zum Datenschutz, Teil 2: Einzelvorschriften des Bundes zum Datenschutz. EDV und Recht, Bd. 10 (Hrsg. Herbert Fiedler), Berlin 1978
(zitiert: Gola/Hümmerich/Kerstan)

GOLL, Eberhard
- Offenbarungsbefugnisse im Rahmen des § 203 II StGB. Zugleich eine Darstellung der verschiedenen Funktionen des Merkmals "unbefugt". Diss. Tübingen 1980

GRASSL, Michael; WEIGERT, Klaus
- Die Neuregelung des Sozialdatenschutzes in: DSWR 1981 S. 113 - 115; S. 140 - 143 und S. 186 - 188
- Die Neuregelung des Sozialdatenschutzes - Zweifelsfragen und Unstimmigkeiten in: DuD 1981 S. 72 - 78

GRELL, Rainer
- Landesdatenschutzgesetz für Baden-Württemberg, Kommentar, Stuttgart 1980

GROEBEN, Wolfgang von der
- Vergleich zwischen dem amerikanischen und dem deutschen Bundesdatenschutzgesetz in: ÖVD 5/1977 S. 17 - 18

GROSSMANN, Gerd
- Die neuen SCHUFA-Klauseln - Überlegungen aus der Sicht eines Kreditinstitutes in: DSWR 1980 S. 278 - 283

GUNZENHÄUSER, Rul
- Informationstheorie und Ästhetik S. 225 - 237 in Kybernetik - Brücke zwischen den Wissenschaften (Hrsg. Helmar Frank) 3. Aufl. Frankfurt/M. 1964

HAEFNER, Klaus
- Der "Große Bruder", Chancen und Gefahren für eine informierte Gesellschaft, Düsseldorf,Wien, 1980

HAFT, Fritjof
- Computerkriminalität und Datenschutz in: DSWR 1979 S. 136 - 142
- Zur Situation des Datenschutzstrafrechts in: NJW 1979 S. 1194 - 1197
- Eigenhändige Delikte in: JA 1979 S. 651 - 658
- Praktische Erfahrungen mit juristischer Rhetorik in: MDR 1980 S. 967 - 980
- Einführung in das juristische Lernen, Bielefeld 1983 (zitiert: Haft, Einführung in das juristische Lernen)
- Strafrecht, Besonderer Teil, München 1982 (zitiert: Haft BT)

HAMMERBACHER, Hans
- Zu den Begriffen "Geheimnis" ("Geheimhaltung") und "Offenbarung" in: DuD 1983 S. 115 - 116
- Die Anonymisierung personenbezogener Daten - Zusammenhänge, Begriffe, Maßnahmen, Ergebnisse - in: DuD 1982 S. 284 - 292

HASE, Friedhelm - Das Recht auf "informationelle Selbstbestimmung"
in: DuR 1984 S. 39 - 47

HEINEMANN, Günter - Datei-Übersicht für Krankenkassen nach § 15 des Bundesdatenschutzgesetzes
in: DOK 1978 S. 412 - 417

HEINZ, Wolfgang - Wirtschaftskriminologische Forschung in der Bundesrepublik Deutschland
in: wistra 1983 S. 128 - 134

HELLER, Richard - Neue Technik - Alte Gesetze. Zur Mitbestimmung bei Personalinformationssystemen S. 46 - 54
in: Datenschutz im Konflikt, Jahrestagung 1982 der Deutschen Vereinigung für den Datenschutz (Hrsg.: Peter Gola), DVR-Beiheft 14, München 1983
(zitiert: Heller, DVD-Tagung 1982)

HELMIG, Ekkehard - Datenschutzprobleme in der Presse - zur Notwendigkeit der Einbeziehung der Presse in den Geltungsumfang des Bundesdatenschutzgesetzes
Diss. Heidelberg 1978

HEMPELMANN, Gernot - Datenschutz und Pressedatenbanken
in: FuR 8/1979 S. 412 - 414

HEMPFER, Walter - Zur Zuständigkeit des Landesbeauftragten für den Datenschutz
in: VBlBW 1982 S. 185 - 190

HENDRIKS, Birger - Das "Medienprivileg" im Rundfunk - Kontroverse Interpretation des publizistischen Vorbehalts -
in: FuR 8/1979 S. 407 - 410

HERDEN, Ewald;
KARRER, Josef - Datenschutz - Organisation und Realisierung bei der Kommunalverwaltung, dargestellt am Beispiel der Stadt Nürnberg
in: VOP 1981 S. 365 - 367 und VOP 1982 S. 30 - 34 u. S. 138 - 145
(zitiert: Herden/Karrer)

HERGENHAHN, Gerhard - Verbreitete Mißverständnisse um das Bundesdatenschutzgesetz
in: DuD 1977 S. 25 - 29

HEROLD, Horst - Polizeiliche Datenverarbeitung und Menschenrecht
in: RuP 1980 S. 79 - 86

HEUSSNER, Hermann - Zur Funktion des Datenschutzes und zur Notwendigkeit bereichsspezifischer Regelungen S. 173 - 200
in: FS für Georg Wannagat ("Im Dienste des Sozialrechts"), Köln 1981
(zitiert: Heussner, FS Wannagat)

HILL, Hermann
- Einführung in die Gesetzgebungslehre, Heidelberg 1982

- Kontinuität im Datenschutz? DANA 5/1982 S. 4 - 5

HÖFER, Helmut; KASPARI, Werner
- Die SCHUFA - Aufbau - Auskunftswesen - Datenschutz und Rechte des Betroffenen S. 163 - 186 in: Handbuch des Datenschutzes 1979/1980 (Hrsg.: Heidi Heilmann und Friedhelm Wolf), Stuttgart 1980

HÖRLE, Ulrich; WRONKA, Georg
- Bundesdatenschutzgesetz - Auswirkungen auf Werbung und Presse, Bonn 1977

HÜMMERICH, Klaus
- Auskünfte zwischen Arbeitgebern über Arbeitnehmer im Lichte des Bundesdatenschutzgesetzes in: DVR 1977 Bd. 6 S. 129 - 139

HÜMMERICH, Klaus; KNIFFKA, Rolf
- Die Entwicklung des Datenschutzrechts im Jahre 1978 in: NJW 1979 S. 1182 - 1189

HUGGER, Werner
- Gesetze - Ihre Vorbereitung, Abfassung und Prüfung, 1. Aufl. Baden-Baden 1983

HUND, Jürgen
- Das Bundesdatenschutzgesetz und seine Auswirkungen (Teile I - IV) in: DSWR 1977 S. 44 - 47, S. 67 - 72, S. 122 - 127, S. 150 - 155

JESCHEK, Hans-Heinrich
- Lehrbuch des Strafrechts, Allgemeiner Teil, 2. Aufl. Berlin 1972

JULICH, Horst
- Informationsverbund Ordnungsbehörden - Polizei S. 149 - 164 in: Polizeiliche Datenverarbeitung, Arbeitstagung des BKA Wiesbaden vom 02. - 5.11.1982, BKA-Vortragsreihe Bd. 28 (Hrsg.: BKA Wiesbaden 1983)

KÄFER, Gerhard
- Probleme des Datenschutzes beim Aufbau des juristischen Informationssystems S. 505 - 516 in: Deutscher Dokumentartag 1979 (Bearb.: von der Laake u. a.) München 1980

KAMLAH, Ruprecht

- Datenschutz und Informationsfreiheit S. 185 - 200
in: Gefährdet die Informationstechnologie unsere Freiheit? Jahrestagung 1979 der Deutschen Vereinigung für Datenschutz (Hrsg.: Thomas Barthel) München 1980
(zitiert: Kamlah, DVD-Jahrestagung)

- Datenschutz - Konfliktlösung ohne Übertreibung S. 59 - 77
in: Datenschutz im Konflikt, Jahrestagung 1982 der Deutschen Vereinigung für Datenschutz (Hrsg.: Peter Gola) DVR-Beiheft 14, München 1983
(zitiert: Kamlah, DVD-Tagung 1982)

KARPEN, Hans-Ulrich

- Die Verweisung als Mittel der Gesetzgebungstechnik, Heft 64 Neue Kölner Rechtswissenschaftliche Abhandlungen, Berlin 1970

KARPENSTEIN, Peter

- Zur Zuständigkeit der Europäischen Gemeinschaft auf dem Gebiete des Datenschutzes S. 889 - 908
in: Gedächtnisschrift für Christoph Sasse, Bd. II (Das Europa der zweiten Generation), Baden-Baden 1981

KARRER, Josef

- Neuregelung des Sozialgeheimnisses zum Schutz der Sozialdaten - Anwendung und erste Auswirkungen für die kommunale Sozialverwaltung -
in: Kommunalpraxis 1981 S. 128 - 129, 154 - 156 und 179 - 180

KERKAU, Hans-Joachim

- Datenschutz steht Strafverfolgung nicht entgegen
in: DuD 1983 S. 109 - 110

KILIAN, Wolfang

- Arbeitsrechtliche Probleme automatisierter Personalinformationssysteme
in: JZ 1977 S. 481 - 486

- Personalinformationssysteme in deutschen Großunternehmen. Ausbaustand und Rechtsprobleme, 2. Aufl. Berlin 1982
(zitiert: Kilian, Personalinformationssysteme)

KINDERMANN, Harald

- Ministerielle Richtlinien der Gesetzestechnik, Berlin 1979
(zitiert: Kindermann)

- Entwicklungsstand legistischer Richtlinien des deutschen Sprachraums S. 211 - 231
in: Theo Öhliger, Methodik der Gesetzgebung: Legistische Richtlinien in Theorie und Praxis, Wien, New York 1982 (= Forschungen aus Staat und Recht, Bd. 57)
(zitiert: Kindermann in: Öhliger, Methodik und Gesetzgebung)

KLEINKNECHT, Theodor - Strafprozeßordnung, Kommentar, 31. Aufl. München 1981

KLUG, Ulrich - Juristische Logik, 4. Aufl. Berlin 1982 (zitiert: Klug, Juristische Logik)

- Zur Problematik juristischer Definitionen S. 199 - 210 in: Gesetzgebungstheorie, Juristische Logik, Zivil- und Prozeßrecht, Gedächtnisschrift für Jürgen Rödig (Hrsg.: U. Klug, Th. Ramm, F. Ritter, B. Schmiedel), Berlin 1978 (zitiert: Klug, Gedächtnisschrift für Rödig)

KRAUSE, Peter - Das Recht auf informationelle Selbstbestimmung - BVerfGE 65,1 in: JuS 1984 S. 268 - 275

KREY, Volker - Zur Verweisung auf EWG-Verordnungen in Blankettstrafgesetzen am Beispiel der Entwürfe eines Dritten und Vierten Gesetzes zur Änderung des Weingesetzes in: EWR 2/1981 S. 109 - 200

KRÖGER, Klaus - Das Datenschutzgesetz im Bereich der öffentlichen Verwaltung nach dem Bundesdatenschutzgesetz in: DÖV 1977 S. 301 - 305

- Bundesdatenschutzgesetz, Beck'sche Textausgabe mit Einführung, München 1980

KUBICA, Klaus - Was wird aus INPOL? in: Kriminalistik 7 - 8/1981 S. 317 - 319

KÜPPERS, Rudolf - Zu den neuen Geheimhaltungs- und Datenschutzvorschriften im Sozialgesetzbuch in: DuD 1980 S. 185 - 190

KÜSTER, Dieter - Das INPOL-System - Zielsetzung und Ausbaustand 1982, S. 57 - 72 in: Polizeiliche Datenverarbeitung, Arbeitstagung des BKA Wiesbaden vom 2. - 5.11.1982, BKA Vortragsreihe BD. 28 (Hrsg.: BKA Wiesbaden) 1983

KUTZMANN, Thomas - Landesdatenschutzgesetz Rheinland-Pfalz, Kommentar (= Kommunale Schriften für Rheinland-Pfalz, Bd. 39), Köln 1982

LACKNER, Karl - Strafgesetzbuch mit Erläuterungen, 12. Aufl. München 1978

LADUGA, Horst - Das Bundesdatenschutzgesetz und seine Anwendung im Reisebüro in: DuD 1978 S. 204 - 206

LAUFER, Hartmut; STEINBRINCK, Tilo
- Keine Panik wegen des Datenschutzes! (Teil 2)
in: online-adl-nachrichten 4/1977 S. 269 - 272
(zitiert: Laufer/Steinbrinck)

LEIB, Hans-Jürgen
- Was ist eine Datei? Anregungen zur praktischen Anwendung eines unpraktischen Begriffs
in: ÖVD 7 - 8/1978 S. 22 - 24

LENCKNER, Theodor
- Wertausfüllungsbedüftige Begriffe im Strafrecht und der Satz "nullum crimen sine lege"
in: JuS 1968 S. 249 - 257 und S. 304 - 310
- Strafgesetzgebung in Vergangenheit und Gegenwart S. 239 - 261
in: Tradition und Fortschritt im Recht, Festschrift gewidmet der Tübinger Juristenfakultät zu ihrem 500jährigen Bestehen von ihren gegenwärtigen Mitgliedern, (Hrsg.: Joachim Gernhuber), Tübingen 1977
(zitiert: Lenckner, Tübinger FS)
- Computerkriminalität und Vermögensdelikte (Schriftenreihe, Juristische Studiengesellschaft Karlsruhe, Heft 149), Karlsruhe 1981
(zitiert: Lenckner, Computerkriminalität)

LEUZE, Ruth; SCHEDLER, Günter; SCHNEIDER, Werner
- Datenschutz und neue Medien
(Gütachten für die Expertenkommission "Neue Medien" der Landesregierung Baden-Württemberg)
in: ÖVD 10/1980 S. 10 - 17
(zitiert: Leuze/Schedler/Schneider)

LILIE, Hans
- Ärztliche Dokumentation und Informationsrechte des Patienten, Recht und Medizin Bd. 5, Frankfurt/M. 1980

LINDEMANN, P.
- Datenschutzrecht (BDSG) und Persönlichkeitsrecht
in: DuD 1979 S. 221 - 224

LOUIS, Hans Walter
- Grundzüge des Datenschutzrechts, Köln 1981

LÜKE, Gerhard
- Registereinsicht und Datenschutz
in: NJW 1983 S. 1407 - 1409

LUX, Helmut
- Bundesdatenschutzgesetz, Personalführung und Personalbearbeitung
in: BWV 1979 S. 276 - 277

MALLMANN, Otto
- Kreditauskunfteien und Datenschutz in den USA
in: AWD 1973 S. 78 - 84
- Datenschutz in Schweden: Das neue Datengesetz
in: ÖVD 1/1974 S. 31 - 33
- Zielfunktionen des Datenschutzes. Schutz der Privatsphäre - korrekte Information.
(= Kybernetik, Datenverarbeitung, Recht Bd. 6, Hrsg.: Spiros Simitis) Frankfurt/M. 1977
(zitiert: O. Mallmann, Zielfunktionen)
- Anmerkungen zu OLG Saarbrücken NJW 1981 S. 136 - 137
in: NJW 1981 S. 137 - 138

MALLMANN, Otto; WALZ, Stefan
- Schutz der Sozialdaten nach dem neuen Sozialgesetzbuch
in: NJW 1981 S.1020 - 1024

MARX, Michael
- Erfaßt das geltende Strafrecht strafwürdige Handlungen aus dem Bereich der Computerkriminalität?
in: DSWR 1977 S. 323 - 325
- Zur Auslegung des Tatbestandsmerkmals "Übermitteln" in § 41 BDSG Abs. 1 Nr. BDSG
in: DSWR 1979 S. 86 - 88

MAUNZ, Theodor; DÜRIG, Günter; HERZOG, Roman
- Grundgesetz, Kommentar, Loseblatt, Stand: 22.Liefg. (Sept. 1983); bearbeitet von Theodor Maunz, Günter Dürig, Roman Herzog, Rupert Scholz, Peter Lerche, Hans-Jürgen Papier, Albrecht Randelzhofer, Eberhard Schmidt-Assmann, München 1958
(zitiert: Maunz/Dürig/Herzog)

MAURER, Michael
- Volksfeste in Ladengeschäften - Zu Verweisungen der Art des § 60 b Abs. 2 GewO
in: GewArch 1982 S. 13 - 17

MEISTER, Herbert
- Bundesdatenschutz oder Datenerhebungs-Ermächtigungsgesetz?
in: ZRP 1979 S. 129 - 133
- Aspekte einer Novellierung des Bundesdatenschutzgesetzes
in: DuD 1980 S. 123 - 127
- Datenschutz im Zivilrecht - Das Recht am eigenen Datum (= Schriftenreihe Recht und Gesellschaft, Bd. 1), 2. Aufl. Bergisch-Gladbach 1981
(zitiert: Meister, Datenschutz)
- Entwicklungen im europäischen Datenrecht
in: RIW/AWD 1982 S. 481 - 489

MIDDENDORF, Wolf
- Kriminologie in Fällen (Polizei aktuell, Bd. 32) Stuttgart 1980

MÜLLER-LUTZ, H. L.
- Das "Datenschutzgesetz" in: VW 1979 S. 907 - 910

NAUCKE, Wolfgang
- Über Generalklauseln und Rechtsanwendung im Strafrecht (Recht und Staat, Heft 417), Tübingen 1973 (zitiert: Naucke (1973))
- Strafrecht - Eine Einführung, (Juristische Lernbücher 3/4), 3. Aufl. Frankfurt/M. 1980 (zitiert: Naucke, Strafrecht)

NEUMANN, Gabriele
- Die Zusammenarbeit der Kriminalpolizei mit Auskunfteien und Detekteien (= Bd. 5 Forschungsreihe Kriminalwissenschaften, Hrsg.: Friedrich Geerds) Lübeck 1980

NOLL, Peter
- Zur Gesetzestechnik des Entwurfs eines Strafgesetzbuches in: JZ 1963 S. 297 - 302
- Gesetzgebungslehre, Reinbek b. Hamburg 1973
- Die Berücksichtigung der Effektivität der Gesetze bei ihrer Schaffung S. 131 - 146 in: Theo Öhliger, Methodik der Gesetzgebung: Legistische Richtlinien in Theorie und Praxis, Wien, New York 1982 (zitiert: Noll, Die Berücksichtigung der Effektivität)

OSSENBÜHL, Fritz
- Die verfassungsrechtliche Zulässigkeit der Verweisung als Mittel der Gesetzgebungstechnik in: DVBl. 1967 S. 401 - 408

OSTENDORF, Heribert
- Die öffentliche Identifizierung von Beschuldigten durch die Strafverfolgungsbehörden als Straftat in: GA 127 (1980) S. 445 - 467

PAWLIKOWSKY, Gerhart
- Was bringt das Österreichische Datenschutzgesetz? in: DuD 1979 S. 22 - 24

PEITZSCH, Wolfram
- Was der Kunde wissen sollte: Datengeheimnis bei Sparkassen - Rechtsfragen des Datenschutzes öffentlich-rechtlicher Kreditanstalten - in: DSWR 1980 S. 29 - 37

RAAB, Erich
- Probleme der Frageformulierung S. 255 - 270 in: Handbuch der Marktforschung, Hrsg.: Karl Christian Behrens, 1. Halbband, Wiesbaden 1974

REISINGER, Leo
- BDSG und DSG - ein Vergleich der deutschen und österreichischen Datenschutzgesetzgebung in: DuD 1979 S. 120 - 125

RIEDEL, Harald
- Empirische Untersuchungen zu einem informationspsychologischen Gedächtnismodell in: GrKG Bd. 8 S. 1 - 13, Quickborn 1967
- Die Bestimmung von Speicherdaten und Zufallskonstanten für ein informationspsychologisches Gedächtnismodell in: GrKG Bd. 8 S. 14 - 22 Quickborn 1967

RIESS, Peter
- Die Rechtsstellung des Verletzten im Strafverfahren, Gutachten C für den 55. Deutschen Juristentag (Hrsg.: Ständige Deputation des Deutschen Juristentages), München 1984 (zitiert: Rieß, Gutachten)

RIHACZEK, Karl
- Datenschutz im Wandel in: DuD 1980 S. 228 - 231

RINGWALD, Gerhard
- Epidemiologische Forschung und Datenschutz in: NJW 1982 S. 2593 - 2595
- Der Datenabruf und das Bundesdatenschutzgesetz in: JZ 1983 S. 291 - 297
- INPOL und StA. Zum Abrufrecht der Staatsanwaltschaft aus polizeilichen Datenspeichern, EDV und Recht, Bd. 14, Berlin 1984

RISCHE, Herbert
- Die Neuregelung des Sozialgeheimnisses in § 35 SGB I und der Schutz der Sozialdaten im SGB X in: DRV 1980 S. 379 - 390

RISSING-VAN SAAN, Ruth
- Privatsphäre und Datenverarbeitung - Ein strafrechtlicher Beitrag zum Datenschutz - Diss. Bochum 1978

RÖDIG, Jürgen
- Logische Kriterien für die korrekte Verwendung von Legaldefinitionen S. 307 - 321 in: Jürgen Rödig, Schriften zur juristischen Logik (Hrsg.: E. Bund, B. Schmiedel, G. Thieler-Mevissen) Berlin 1980 (zitiert: Rödig, Schriften zur juristischen Logik)

ROOS, Gerhard
- Entkriminalisierungstendenzen im Besonderen Teil des Strafrechts (Europäische Hochschulschriften: Reihe 2, Rechtswiss.; Bd. 276), Frankfurt/M. 1981

RUCKRIEGEL, Werner
- Die Sprache, das "Haus des Seins"? in: ÖVD 7/8/1981 S. 3 - 6

RUCKRIEGEL, Werner; GROEBEN, Wolfgang von der; HUNSCHE, Burkhard
- Datenschutz und Datenverarbeitung in Nordrhein-Westfalen, Kommentar, Köln 1979 (zitiert: Ruckriegel u. a.)

RUMPF, Hartmut
- Zur Novellierung des BDSG in: DSWR 1982 S. 127 - 134

SACHAU, Manfred
- Die Entwicklung des Datenschutzrechts - Auswirkungen im kommunalen Bereich in: Der Bayerische Bürgermeister 2/1981 S. 16 - 18

SASSE, Christoph
- Das BDSG - Licht und Schatten S. 75 - 87 in: Aktuelle Beiträge über den Datenschutz, Schriftenreihe Schimmelpfeng, Bd. 9, Frankfurt/M. 1977

SAVIGNY, Eike von
- Grundkurs im wissenschaftlichen Definieren, 2. Aufl. München 1971

SCHALL, Hero
- Auslegungsfragen des § 179 StGB und das Problem der eigenhändigen Delikte in: JuS 1979 S. 104 - 110

SCHEDL, Ilse
- Bundesdatenschutzgesetz. Ein praktischer Leitfaden für alle Betriebe, Behörden und freie Berufe, 1. Aufl. Kissing 1977
- Kritische Anmerkungen zum neuen Bundes-Datenschutzgesetz in: DSWR 1977 S. 180 - 183
- Randbemerkungen zum 10. Buch des Sozialgesetzbuches (SGB X) in: DSWR 1983 S. 283 - 284

SCHIMMEL, Wolfgang
- Datenschutz S. 145 - 167 in: ADV und Recht, Einführung in die Rechtsinformatik und das Recht der Informationsverarbeitung, 2. Aufl. Berlin 1976 (JA-Sonderheft 6), (zitiert: Schimmel, ADV und Recht)

SCHINDEL, Jost
- Das amerikanische Datenschutzgesetz von 1974 - Deutsche Übersetzung mit kurzer Einführung (Beiträge zum Datenschutz, Heft 3, Hrsg.: Hessischer Datenschutzbeauftragter), Wiesbaden 1975

- Das französische Datenschutzgesetz vom 6.1.1978 - eine bürgerfreundliche Regelung in: DSWR 1978 S. 232 - 235

SCHLAPP, Thomas - Zur Einführung: Logik und Recht in: JuS 1984 S. 505 - 509

SCHMID, Hans - Ein Überblick über das Landesdatenschutzgesetz in: Das Polizeiblatt für das Land Baden-Württemberg 1980 S. 82 - 86

SCHNEIDER, Jochen; STEINBRUNCK, Tilo - Was ist "Übermitteln"? Vorläufige Verwaltungsvorschriften lassen Fragen offen! online-adl-nachrichten 6/1979 S. 478

- Datenschutz und Neue Medien in: NJW 1984 S. 390 - 398

SCHNELL, Angelika - §§ 67 - 69 WeinG - nulla poena sine lege? Dissertation Tübingen 1985 (in Vorbereitung)

SCHOMERUS, Rudolf - Datenschutz in den Vereinigten Staaten in: ÖVD 11/1977 S. 3 - 7

- Das französische Datenschutzgesetz in: DuD 1978 S. 61 - 63

- Zum Stand des Datenschutzes in den USA in: DVR 1981 S. 231 - 242

- Datenschutz oder Datenverkehrsordnung in: ZRP 1981 S. 292 - 294

SCHÖNKE, Adolf; SCHRÖDER, Horst - Strafgesetzbuch, Kommentar, 21. Aufl. München 1982; begründet von Adolf Schönke, fortgeführt von Horst Schröder, bearbeitet von Theodor Lenckner, Peter Cramer, Albin Eser und Walter Stree (zitiert: Schönke-Schröder)

SCHOTT, Frieder - Der Mikrofilm: Ein modernes Kommunikationsmittel in: DSWR 1983 S. 21 - 30

SCHÜNEMANN, Bernd - Nulla poena sine lege? Rechtstheoretische und verfassungsrechtliche Implikationen im Strafrecht, Berlin 1978

- Der strafrechtliche Schutz von Privatgeheimnissen in: ZStW 90 (1978) S. 11 - 63

SCHULZ, Gerhard - Orientierungshilfe zum Bundesdatenschutzgesetz in: BKK 1978 S. 57 - 60

SCHWAPPACH, Jürgen - Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (BDSG) erläutert von Jürgen Schwappach, Bergisch-Gladbach 1977

SCHWEINOCH, Joachim; GEIGER, Hansjörg
- Bayerisches Datenschutzgesetz, Kommentar, Köln 1978

SCHWEIZER, Rainer J.
- Der Stand der Datenschutzgesetzgebung in der Schweiz
in: DuD 1980 S. 153 - 156

- Das Muster-Datenschutzgesetz für die schweizerischen Kantone
in: DuD 1983 S. 202 - 207

SCHWEIZER, Robert
- Kernprobleme des Bundesdatenschutzgesetzes
Teil I in: DB 1977 S. 289 - 294
Teil II in: DB 1977 S. 337 - 339

SEIBERT, Thomas-Michael
- Aktenanalysen - Zur Schriftform juristischer Deutungen (Bd. 3 der Reihe "Kommunikation und Institution") Tübingen 1981

SENDLER, Hans
- Rechtsprobleme personenbezogener Datenverarbeitung im öffentlichen und privaten Bereich - Ein Beitrag zur Auslegung des BDSG -
in: DuD 1977 S. 59 - 65

SIEBER, Ulrich
- Computerkriminalität und Strafrecht, 2. Aufl. Köln 1980
(zitiert: Sieber, Computerkriminalität)

SIEGLERSCHMIDT, Hellmut
- Zweiter Bericht über den Schutz der Rechte des einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der Datenverarbeitung
in: DuD 1981 S. 226 - 238

SIMITIS, Spiros
- BDSG - Ende der Diskussion oder Neubeginn?
in: NJW 1977 S. 729 - 737

- Zur Verwertung von Arbeitnehmerdaten für publizistische Zwecke - Einfluß und Grenzen des Datenschutzes S. 319 - 344
in: Presserecht und Pressefreiheit, Festschrift für Martin Löffler zum 75. Geburtstag, München 1980
(zitiert: Simitis, FS Löffler)

- Datenschutz: Von der legislatorischen Entscheidung zur richterlichen Interpretation
in: NJW 1981 S. 1697 - 1701

- Datenschutz: Erfahrungen und Perspektiven
in: VersR 1981 S. 197 - 207

- Zur Verwertung von Arbeitnehmerdaten für publizistische Zwecke - Einfluß und Grenzen des Datenschutzes
in: DuD 1982 S. 241 - 251

- Die informationelle Selbstbestimmung - Grundbedingung einer verfassungskonformen Informationsordnung
in: NJW 1984 S. 398 - 405

SIMITIS, Spiros;
DAMMANN, Ulrich;
MALLMANN, Otto;
REH, Hans-Joachim
- Kommentar zum Bundesdatenschutzgesetz
3. Aufl. Baden-Baden 1981
(zitiert: Simitis/D/M/R)

SIMON, Jürgen
- Zur Problematik der Einwilligung in die Verarbeitung von Daten bei Wirtschaftsdiensten
in: DANA 1/1982 S. 18 - 20

SIMON, Jürgen;
TAEGER, Jürgen
- Rasterfahndung - Entwicklung, Inhalt und Grenzen einer kriminalpolizeilichen Fahndungsmethode, 1. Aufl. Baden-Baden 1981

- Grenzen kriminalpolizeilicher Rasterfahndung
in: JZ 1982 S. 140 - 145

STAATS, Johann Friedrich
- Zur Problematik bundesrechtlicher Verweisungen auf Regelungen privatrechtlicher Verbände
in: ZRP 1978 S. 59 - 62

STADLER, Gerhard
- Erste Verwaltungserfahrungen mit dem Privacy Act der USA
in: ÖVD 1/2/1977 S. 17 - 19

- Der Bericht der britischen Datenschutzkommission 1978
in: ÖVD 5/1979 S. 11 - 12

- Das französische Datenschutzgesetz vom 6. Jan. 1978
in: ÖVD 4/1979 S. 22 - 23

- Das Österreichische Datenschutzgesetz
in: ÖVD 11/1978 S. 8 - 10

- Vom Datenschutz zur Informationspolitik?
in: DuD 1981 S. 5 - 9

STEFFEN, Wiebke
- Grenzen und Möglichkeiten der Verwendung von Strafakten als Grundlage kriminologischer Forschung: Methodische Probleme und Anwendungsbeispiele S. 89 - 108
in: Historisch-Sozialwissenschaftliche Forschungen, Hrsg.: Paul J. Müller, Die Analyse prozeßorientierter Daten, Stuttgart 1977

STEINKE, Wolfgang
- Kriminalität durch Beeinflussung von Rechnerabläufen
in: NStZ 1984 S. 295 - 297

STEINMÜLLER, Wilhelm

- Der Schutz "medizinischer" Daten: Terminologische, rechtliche und organisatorische Aspekte; sowie ein Vorschlag zur gesetzlichen Regelung des Datenschutzes bei Forschung und Planung S. 135 - 148
in: Medizinische Informatik und Statistik, Bd. 12, 1979
(zitiert: Steinmüller, Der Schutz medizinischer Daten)

- Sicherheitsbereich, Bürgerrecht und Datenkontrolle S. 35 - 61
in: Datenschutz ist Bürgerrecht, Jahrestagung der Deutschen Vereinigung für Datenschutz (Hrsg.: Thomas Barthel und Wilhelm Steinmüller) München 1980
(zitiert: Steinmüller, DVD-Jahrestagung)

SUPPES, Rainer

- Hessisches Datenschutzgesetz, Kommentar, Köln 1982

TEGTMEYER, Henning

- Der Strafantrag nach den Strafvorschriften der Datenschutzgesetze
in: ÖVD 1981 S. 12 - 14

TIEDEMANN, Klaus

- Tatbestandsfunktionen im Nebenstrafrecht, Tübinger rechtswissenschaftliche Abhandlungen, Bd. 27, Tübingen 1969
(zitiert: Tiedemann, Tatbestandsfunktionen)

- Strafbare Erschleichung von Investitionszulagen durch Aufhebung und Neuabschluß von Lieferverträgen?
in: NJW 1980 S. 1557 - 1560

- Datenübermittlung als Straftatbestand
in: NJW 1981 S. 945 - 952

TÖNNIES, J. G.

- Das Zusammenwirken von Datenschutz- und Betriebsverfassungsgesetz
in: DuD 1981 S. 24 - 28

TUBIES, Helga

- Amtshilfe und Datenschutz
in: DuD 1979 S. 75 - 80

- Datenübermittlung innerhalb von Behörden
in: DuD 1979 S. 157 - 162

- Unbestimmte Rechtsbegriffe im Bundesdatenschutzgesetz
in: DuD 1981 S. 148 - 154

TUNER, Lotte

- Datenschutzrichtlinien für die Schweizerische Bundesverwaltung
in: DANA 2/3/1982 S. 7 - 8

UCKERMANN, Eckhart Freiherr von - BDSG: Fragen der Haftung und des Versicherungsschutzes in: DuD 1978 S. 64 - 69

UNGNADE, Dieter - Das Datenschutzgesetz und die Banken in: Zeitschrift für das gesamte Kreditwesen 1979 S. 53 - 58

VESTER, Frederic - Denken, Lernen, Vergessen. Stuttgart 1975

VOSS, Heinz-Rudolf - SCHUFA und Bundesdatenschutzgesetz in: DuD 1979 S. 183 - 187

WARDA, Günter - Strafrechtliche Irrtumslehre (4. Teil) in: JURA 1979 S. 286 - 297

WEISE, Karl-Theodor - Textverarbeitung und Datenschutz in: DuD 1980 S. 139 - 145

- Datenschutz oder Datenverkehrsordnung - eine Alternative? in: DuD 1983 S. 69 - 70

WELTNER, Klaus - Informationstheorie und Erziehungswissenschaft Quickborn 1970 (zitiert: Weltner, Informationstheorie)

WENDER, Karl Friedrich; COLONIUS, Hans; SCHULZE, Hans-Henning - Modelle des menschlichen Gedächtnisses (Kohlhammer-Standards Psychologie) Stuttgart 1980

WIELINGER, Gerhart - Bedingungen der Vollziehbarkeit von Gesetzen S. 154 - 166 in: Theo Öhlinger, Methodik der Gesetzgebung: Legistische Richtlinien in Theorie und Praxis, Wien, New York 1982 (= Forschungen aus Staat und Recht, Bd. 57) (zitiert: Wielinger)

WIESE, Walter - Zur Neuordnung des Schutzes der Sozialdaten in: ÖVD 4/1981 S. 11 - 17

WIMMER, Sigmund - Datenschutz in der öffentlichen Verwaltung S. 61 - 68 in: Datenschutzrecht und - praxis im Zeichen der BDSG-Novellierung: Tagungsband; Referate und Ergebnisse 6. DAFTA, 27. - 29.10.1982 (Hrsg.: Hans Gliess), 1. Aufl. Köln 1983

WISSEL, Holger; WRONKA, Georg - Neuere Tendenzen im Datenschutz - Auswirkungen auf Presse und Werbung - in: AfP 1980 S. 133 - 140

WITTKÄMPER, G. W. - Datenoasen - ein Mythologem?
in: DuD 1978 S. 59 - 60

WOCHNER, Manfred - Das Datenschutzdurcheinander
in: DVBl 1982 S. 233 - 241

WOERTGE, Hans-Georg - Die Prinzipien des Datenschutzrechts und ihre Realisierung im geltenden Recht, Heidelberg 1984

WOHLGEMUTH, Hans H. - Datenschutz für Arbeitnehmer. Eine systematische Darstellung, Neuwied 1983

WRONKA, Georg - Datenschutz und Medienprivileg
in: FuR 1979 S. 123 - 124

ZIEGLER-JUNG, Bärbel - Einführung in die Datenschutzfragen im IuD-Bereich unter besonderer Berücksichtigung der Problematik bei medizinischer Information und Dokumentation, S. 477 - 488
in: Deutscher Dokumentartag, Willingen/Hochsauerland 1979; Bearb. von: Mathilde von der Laake, Hilde Strohl-Goebel, 1980
(zitiert: Ziegler-Jung, Datenschutzfragen)

ZIELINSKI, Diethart - Das legislatorische Problem "Datenschutz" aus strafrechtlicher Sicht, S. 129 - 154
in: Datenschutz. Juristische Grundsatzfragen beim Einsatz elektronischer Datenverarbeitungsanlagen in Wirtschaft und Verwaltung. Hrsg.: Wolfgang Kilian, Klaus Lenk, Wilhelm Steinmüller) Frankfurt/M. 1973

ZÖLLNER, Wolfgang - Die Nutzung DV-gestützter Personalinformationssysteme im Schnittpunkt von Datenschutzrecht und Betriebsverfassung
in: DB 1984 S. 241 - 246

Ohne Verfasserangabe:

- Arbeitskreis "Datenschutz" der Spitzenorganisationen der Wirtschaft.

- Beiträge zu Auslegungsproblemen des BDSG. Bergisch-Gladbach. Teil I: 1978, Teil II 1979
(zitiert: Arbeitskreis Teil I bzw. Teil II)

- Auswirkungen des Datenschutzes: Eine Studie zum Datenschutz aufgrund eines Projektes der GMD. Hrsg.: Gesellschaft für Mathematik und Datenverarbeitung mbH, Bonn, Institut für Datenverarbeitung im Rechtswesen (IDR), München 1979
(zitiert: GMD-Studie)

- Anspruch des Bürgers auf Datenkontrolle. Bundesinnenminister Gerhart Baum in einem Interview mit dem Münchner Merkur
in: FuR 4/1979 S. 216 - 218
(zitiert: Baum FuR 1979)

- Den Datenschutz aus der Konfrontation führen. Ein Online-Gespräch mit dem Bundesdatenschutzbeauftragten Reinhold Baumann
in: ÖVD 1983 S. 104 - 108
(zitiert: R. Baumann, ÖVD 1983)

- Deutscher Juristentag: Grundsätze für eine gesetzliche Regelung des Datenschutzes, Bericht der Datenschutzkommission des Deutschen Juristentages, München 1974
(zitiert: Datenschutzkommission des Deutschen Juristentages)

- Gefährdet die Informationstechnologie unsere Freiheit? Jahrestagung 1979 der Deutschen Vereinigung für Datenschutz (Hrsg.: Thomas Barthel)
München Wien 1980
(zitiert: DVD-Jahrestagung 1979)

§ 1

EINLEITUNG

"Datenschutz" ist ein Schlagwort, das seit einigen Jahren, und nicht nur durch das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz oder durch die Bestrebungen, einen neuen maschinenlesbaren Personalausweis einzuführen, in der politischen und juristischen Diskussion steht [1]. In der öffentlichen Meinung wird dabei der Begriff "Datenschutz" sehr weit gefaßt: Jede Erlangung, Speicherung oder Weitergabe von Informationen und jede Mißachtung von Geheimnisvorschriften gilt als Verstoß gegen "das Datenschutzgesetz". Dabei existiert "das Datenschutzgesetz" überhaupt nicht, sondern es wurden, was häufig übersehen wird, ein Bundesdatenschutzgesetz und elf Landesdatenschutzgesetze erlassen [2]. Nur der Verstoß gegen eine der in diesen zwölf Datenschutzgesetzen statuierten Strafnormen rechtfertigt es, von einer "Datenschutzkriminalität im eigentlichen Sinne" zu sprechen.

Da der Begriff "Datenschutz" selbst von vielen Juristen unpräzise verwandt wird, soll vor einer Festlegung und Eingrenzung des Untersuchungsgegenstandes und des Zweckes der Arbeit eine Begriffsklärung erfolgen: Als Datenschutzkriminalität im weiteren Sinne sind alle Verstöße gegen die Sanktionsnormen zu verstehen, deren Handlungsobjekt "Daten" sind.

1) Der Begriff "Datenschutz" hat sich zwar durchgesetzt, ist aber mißglückt, da es nicht um den Schutz der Daten (das wäre "Datensicherung"), sondern des Menschen geht, weshalb "Verdatungsschutz" exakter wäre: vgl. Fiedler in: Steinmüller, Informationsrecht S. 194; ähnlich Gola DSWR 1983, 95. Eine Erklärung für die heutige Terminologie gibt Schimmel, ADV und Recht, S. 145: "Die Bezeichnung 'Daten'-Schutz ist aus der Nähe des Problembereichs Datenschutz zur automatischen 'Daten'-Verarbeitung entstanden. Daten wird hier aber untechnisch im Sinne von Informationen gebraucht." Dazu auch Ringwald, INPOL und StA, § 2 I. 1.a) FN 5.

2) Die Abgrenzung wird grds. nur im Bereich der öffentl. Verwaltung relevant. Näheres dazu in § 3 der Arbeit.

Somit fällt darunter nicht nur ein Verstoß gegen eine Strafnorm der "eigentlichen" Datenschutzgesetze, sondern z. B. auch die Verletzungen des persönlichen Lebens- und Geheimbereichs (§§ 201 ff. StGB), die Verletzung des Dienstgeheimnisses (§ 353 b StGB) oder der Geschäftsgeheimnisverrat (§ 17 UWG). Weiter erfaßt dieser - von der öffentlichen Meinung geprägte - "weite" Datenschutzbegriff die verschiedenen Formen der Computerkriminalität [3] (Computermanipulation, -sabotage und -spionage, sowie Rechenzeitdiebstahl) [4]. Demgegenüber sollte exakterweise von einer Datenschutz-Kriminalität im eigentlichen Sinne nur dann gesprochen werden, wenn ein Verstoß gegen die Sanktionsnormen des Bundes- und der elf Landesdatenschutzgesetze vorliegt.

Die vorliegende Arbeit beschränkt sich auf diese Verstöße gegen die Datenschutzgesetze im eigentlichen Sinn. Nicht erörtert wird die Computerkriminalität. Deren Zielrichtung ist das Vermögen [5]. Aufgabe der Datenschutzgesetze jedoch ist, "der Beeinträchtigung schutzwürdiger Belange des Betroffenen entgegenzuwirken" [6], worunter primär der Bereich der Persönlichkeitssphäre verstanden wird.[7] Ausgeklammert ist auch das dogmatische Verhältnis zu § 203 StGB [8]. Dies muß einer anderen Untersuchung vorbehalten bleiben.

3) Die Reichweite des Begriffes ist umstritten. Hier ist mit Sieber, Computerkriminalität, S. 188; Kamlah in: Burhenne/Perband § 41 RN 6; Schneider in: Galiwas/S/S § 41 RN 20; Göppinger,Kriminologie, S. 669 f.; Marx DSWR 1977, 325 Anm. 1; Steinke NStZ 1984, 295 und Haft DSWR 1979, 136 davon auszugehen, daß unter die Computerkriminalität jedenfalls nicht die Verstöße gegen die hier erörterten zwölf Datenschutzgesetze fallen.

4) Geiger/Schneider, S. 196; Göppinger, Kriminologie S. 670 f.; Lenckner, Computerkriminalität, S. 20; Sieber, Computerkriminalität, S. 188 und Bauknecht S. 105.

5) Vgl. dazu die Arbeit von Sieber, Computerkriminalität und Strafrecht, 2. Aufl. 1980, die auch empirisch ausgerichtet ist.

6) § 1 BDSG und alle Landesdatenschutzgesetze.

7) Auernhammer, Kommentar, Einführung RN 31; nach Simitis in: Simitis/D/M/R Einleitung, RN 31, soll die "Privatsphäre" geschützt werden; ebenso die Gesetzesbegründung (BT-Drs. 7/1027 S. 14 f.).

8) Zum Konkurrenzverhältnis dieser Delikte: Schönke-Schröder-Lenckner, § 203 RN 46 und 76; sowie Dreher/Tröndle, § 203 StGB RN 9a und 33 (beide jeweils mwN).

Untersucht werden sollte in erster Linie, ob die komplizierte Verweisungstechnik in § 41 BDSG (bzw. den Datenschutzgesetzen der Länder) zu Fehlern in der Rechtsanwendung geführt hat. Auf den ersten Blick scheint § 41 BDSG nämlich einfach handhabbar, bei näherer Betrachtung indessen erweist er sich wenig praxisgerecht, da er auf einem System komplexer Verweisungen basiert. Es wurden deshalb zunächst die datenschutzrechtlichen Sanktionsnormen in ihre Bestandteile aufgelöst und dann - den einzelnen Tatbestandsmerkmalen folgend - untersucht, inwieweit die Strafverfolgungsbehörden in der Praxis mit diesen "verweisungsgeprägten" Strafvorschriften fertiggeworden sind. Zwangsläufig mußte die Arbeit somit (auch) empirisch sein.

Da bisher fast kaum Urteile von Strafgerichten vorliegen, habe ich auf die Ermittlungsverfahren zurückgegriffen und war bestrebt, alle Verfahren zu erfassen, die in den ersten fünf Jahren seit Inkrafttreten des BDSG [9], also von 1978 bis 1982, eingeleitet wurden. Bis auf wenige Ausnahmen gelang dies auch, so daß schließlich 159 Ermittlungsvorgänge analysiert werden konnten. Die Auswertung dieses Aktenmaterials aus der ganzen Bundesrepublik bildet den Schwerpunkt der Arbeit, so daß die Rechtstatsachen und nicht die Rechtsbegriffe im Vordergrund stehen. Die Arbeit will aber nicht nur Problematik von Verweisungen aufgrund einer empirischen Untersuchung der Datenschutz-Kriminalität erörtern, sondern zugleich auch die Ergebnisse dieser "Quellenforschung" darstellen [10]. Basierend darauf ist dann eine weitere wissenschaftliche Erforschung des Datenschutz-Strafrechts möglich [11], das jedoch nur insoweit hier behandelt wird, als es für die Analyse unumgänglich ist. Es werden deshalb im Rahmen der Auswertung und im Anhang über 60 Verfahren, teils in Kurzfassung, teils ausführlich vorgestellt; dabei handelt es sich bis auf zwei Verfahren um bisher unveröffentlichtes Material.

9) Gemäß § 47 BDSG trat das Gesetz am 1.1.1978 in Kraft.

10) Vgl. dazu insbesondere § 4 der Arbeit.

11) So z. B. die Erörterung des Verhältnisses von § 203 StGB und § 41 BDSG anhand praktischer Fälle.

Die Literatur zur allgemeinen Datenschutzproblematik liegt inzwischen in "kaum noch überschaubarer Fülle" vor [12]. Da die Strafbestimmungen Verstöße gegen die jeweiligen Regelungen statuieren, hatte dies zwangsläufig auch Auswirkungen auf die strafrechtlich relevanten Fragen. Ich habe dennoch versucht, die bis Anfang 1984 veröffentlichten Meinungen zu berücksichtigen. Gleiches gilt für die Rechtsprechung, so daß auch das Urteil des BVerfG vom 15.12.1983 zum Volkszählungsgesetz [13] noch mit einbezogen werden konnte.

Die Arbeit beginnt in § 2 mit einem Überblick über die Geschichte der Datenschutzgesetzgebung, insbesondere der Entstehung der Strafnorm des Bundesdatenschutzgesetzes (§ 41 BDSG). Nach der Darstellung der weiteren Entwicklung auf dem Gebiet des Datenschutzrechts in der Zeit nach der Verabschiedung des BDSG werden die Lösungsversuche ausländischer Staaten dargestellt, wobei auf eine ausführliche Kommentierung und Stellungnahme verzichtet wird. Dies würde den Umfang der Arbeit übersteigen.

Im § 3 werden die Verweisungen der Datenschutzgesetze vorgestellt. Nach einer kurzen Erläuterung der Verweisungstechnik und Klassifizierung der verschiedenen Verweisungsarten werden die Verweisungen des BDGB analysiert und graphisch dargestellt. Dabei wird sowohl die Komplexität der Regelungen deutlich werden, als auch die hohe Verweisungsintensität bestimmter Bereiche. In einem Exkurs wird exemplarisch gezeigt, wie in einem bereichspezifischen Gesetz (SGB X) im Hinblick auf die Strafbarkeit auf § 41 BDSG verwiesen wird.

12) So Auernhammer, Kommentar, Vorwort zur 2. Aufl., Seite V. Ähnlich Meister, Datenschutz, S. 15 Fn. 2 und Haft DSWR 1979, 141.

13) BVerfGE 65, 1 ff. Das Urteil ist auch abgedruckt in der Beilage 56/83 des Bundesanzeigers vom 24.12.1983 (Nr. 241a) und in NJW 1984, 419-428.

Die nachfolgenden Abschnitte der Arbeit befassen sich mit den Auswirkungen der komplexen Verweisungstechnik der Datenschutzgesetze. Es wird untersucht, inwieweit die komplizierte Datenschutzgesetzgebung zu Fehlern in der Arbeit der Strafverfolgungsbehörden geführt hat.

Dabei werden zuerst in § 4 die Grundlagen und Methodik der empirischen Auswertung erläutert. Es wird dargelegt, wie die Akten erlangt und aufgrund welcher Untersuchungsmethode sie in welcher Weise untersucht wurden. In diesem Rahmen erfolgt auch eine kurze Darstellung der Eigenheiten der Aktenfälle in verfahrensmäßiger Hinsicht, um die Art des verarbeiteten Materials im Hinblick auf seine "Qualität" besser einschätzen zu können.

Die Auswertung der Wirkungen der Verweisungsketten auf die Rechtsanwendung orientiert sich bei der Gliederung an den einzelnen Tatbestandsmerkmalen des § 41 BDSG und beginnt in § 5 mit der Frage des Schutzbereichs der Datenschutzgesetze. Da diese nur anwendbar sind, wenn eine "Datei" betroffen ist, wird untersucht, wie mit diesem Begriff und den damit zusammenhängenden Problemen von den Strafverfolgungsbehörden verfahren wurde. Ferner wird die Behandlung der Ausnahmeregelungen für den Bereich der Medien und der sog. "internen Daten" analysiert.

Im § 6 werden einerseits die mit dem Begriff "personenbezogene Daten" zusammenhängenden Probleme und Verweisungsschwierigkeiten erörtert, andererseits die der offenkundigen Daten.

Die Auswertung wird mit der Behandlung der einzelnen Tatmodalitäten in § 7 fortgesetzt.

Den letzten Auswertungskomplex bildet in § 8 die Strafantragsproblematik. Da keine eindeutige Verweisung auf einen Antragsberechtigten vorliegt und nach einigen Landesdatenschutzgesetzen auch der Landesdatenschutzbeauftragte ein Antragsrecht besitzt, wird hier die Behandlung dieser Fragen durch die Strafverfolgungsbehörden analysiert.

Die Arbeit endet mit § 9, in dem eine zusammenfassende Würdigung erfolgt und allgemeine Reformvorschläge zu den Datenschutzgesetzen gemacht werden. Zum Abschluß wird ein eigener strafrechtlicher Vorschlag gemacht.

Zu danken ist hier den Justiz- und Innenministerien der Länder, dem Bundeskriminalamt und den Landeskriminalämtern, den Polizeibehörden und besonders den Staatsanwaltschaften, durch deren Hilfsbereitschaft es erst möglich war, das Aktenmaterial zu erlangen und auszuwerten. Ausdrücklich genannt seien die für das Datenschutzstrafrecht zuständigen Referenten der Staatsanwaltschaft Stuttgart, Herr Staatsanwalt Dr. Schulz und sein Nachfolger, Herr Staatsanwalt Dr. Schairer. Zu danken ist auch Herrn Manfred Gerblinger und Herrn Dr. Gerhard Ringwald für Ihre Anregungen.

§ 2

Die Datenschutzgesetzgebung

A) Die Entwicklung in der Bundesrepublik Deutschland

Mit der Verkündung des Bundesdatenschutzgesetzes im Bundesgesetzblatt am 1.2.1977 wurde die Diskussion um die rechtlichen Folgen der Einführung von ADV-Anlagen vorläufig abgeschlossen. Gab es nach einem Bericht der Bundesregierung [2] Ende 1957 im ganzen Bundesgebiet nur 21 ADV-Anlagen, so waren 1968 im öffentlichen und privaten Bereich bereits 3 863 Anlagen eingerichtet und 1 607 bestellt. Nach einer Statistik der Diebold GmbH waren 1970 28 400 Büro-Computer und 11 700 Standard-Computer installiert. 1980 waren es bereits 58 900 Büro-Computer und 14 470 Standard-Computer. Anfang 1983 lag der Bestand an Mikrocomputern bei 304 000. Für 1985 wird mit 405 600 Bürocomputern und 16 390 Standard-Computern gerechnet und für 1988 mit 2,6 Mio. Mikrocomputern [3].

I) Der parlamentarische Beginn der Datenschutzdiskussion

Die parlamentarische Behandlung der mit der automatischen Datenverarbeitung zusammenhängenden Fragen begann zunächst mit den (mehr technischen) Fragen der Anwendung der ADV in der Bundesverwaltung [4] und dem Aufbau regionaler Großrechenzentren [5]. Rasch kamen dann auch die Auswirkungen auf die

1) BGBl. I 1977 S.201.

2) BT-Drs. V/3355 S. 2.

3) "computer zeitung" vom 21.9.1983 S. 6 und Schreiben der Diebold Deutschland GmbH, Frankfurt, an den Verfasser vom 17.3.1983 SW/mt.

4) Nach Beschluß des Bundestages vom 13.12.1967 (BT-Drs. V/2381) folgte der 1. Bericht der Bundesregierung am 7.10.1968 (BT-Drs. V/3355).

5) BT-Drs. V/4308 und V/4546.

Privatsphäre und deren Schutz zur Sprache [6]. Zwar stellte der Bundesminister des Innern noch in seinem Bericht vom 17.4.1970 fest, daß "der Schutz der Privatspäre des Staatsbürgers gegen Eingriffe und Mißbräuche beim Betrieb von automatischen Informationssystemen der öffentlichen Verwaltung ausreichend gesichert sei", gleichwohl aber würde die Notwendigkeit spezieller gesetzgeberischer Maßnahmen geprüft [7].

Wenige Monate später wurde dann im Rahmen der Antwort auf eine kleine Anfrage, in welcher nach den Gesetzgebungskompetenzen des Bundes hinsichtlich des Schutzes der Privatsphäre gefragt worden war, vom Bundesinnenminister mitgeteilt, daß die Bundesregierung hoffe, im Laufe des Jahres 1971 eine Gesetzesvorlage einbringen zu können [8].

II) Die ersten Gesetzesentwürfe auf Bundesebene

Am 2.12.1971 legten Abgeordnete der interparlamentarischen Arbeitsgemeinschaft dem Bundestag den Entwurf eines "Gesetzes zum Schutz vor unbefugter Verwendung personenbezogener Daten (Datenschutzgesetz)" vor (IPA-Entwurf) [9]. Danach sollten vom Datenschutz alle für Zwecke der herkömmlichen und der maschinentechnischen Datenverarbeitung erstellte Unterlagen, insbesondere alle gespeicherten personenbezogenen Daten und die Ergebnisse ihrer Verarbeitung, erfaßt werden (§ 1 IPA-Entwurf). Er erhielt die folgende detaillierte Strafnorm:

§ 24 IPA-Entwurf:

1) Mit Freiheitsstrafe bis zu einem Jahr und mit Geldstrafe oder mit einer dieser Strafen wird bestraft, wer

6) 5. Wahlperiode, 226. Sitzung, 28.3.1969 Anlage 3, Umdruck 631 BT-Drs. VI/648 (2. Bericht, S. 20).

7) BT-Drs. VI/648 S. 21.

8) BT-Drs. VI/1223 vom 5.10.1970 (S. 4).

9) BT-Drs. VI/2885.

a) personenbezogene Daten, die ihm im Zusammenhang mit der Datenverarbeitung bekanntgeworden sind, unbefugt offenbart oder verwertet,

b) den Zugriff auf solche Daten unbefugt gewährt,

c) Datenleitungen anzapft, um den Datentransport zu stören oder Daten unbefugt abzurufen,

d) Programme einführt, die Informationen so speichern und wiederauffinden, daß sie dem ursprünglichen bei der Anmeldung genannten Zweck zuwiderlaufen,

e) die in der Datenbank gespeicherten Daten zu anderen als den im Register verzeichneten Zwecken verwendet oder dies zuläßt.

(2) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer in Kenntnis ihres rechtswidrigen Erwerbs Informationen, die nach Absatz 1 in strafbarer Weise erlangt wurden, entgegennimmt, verwendet, bearbeitet oder in sonstiger Weise darüber verfügt.

(3) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einem anderen einen Vermögensvorteil zu verschaffen, so ist die Strafe Freiheitsstrafe bis zu drei Jahren; daneben kann auf Geldstrafe erkannt werden. Ebenso wird bestraft, wer fremde personenbezogene Daten, die ihm in seiner Eigenschaft als Angehöriger oder Beauftragter der Aufsichtsbehörde bekanntgeworden sind, unbefugt verwertet.

Der IPA-Entwurf wurde jedoch im Bundestag nicht weiter behandelt [10] und auch in der nächsten Legislaturperiode nicht erneut eingebracht. Am 7.9.1972 antwortete die Bundesregierung [11] auf eine kleine Anfrage [12], die wiederum den Schutz der Privatsphäre zum Gegenstand hatte und veröffentlichte gleichzeitig ein Gutachten des Bundesinnenministeriums zur Frage des Datenschutzes [13]. Dort wurde auch zur Problematik von Strafnormen Stellung genommen. Das "Rechtsgut der freien Selbstbestimmung über Individualinformationen" sei zu schützen. Dies habe in der Weise zu geschehen, daß man das rechtswidrige Speichern und Weitergeben von Individualinformationen, das Abgeben an Dritte, ohne selbst die Informationen zu verarbeiten

10) Grund war wohl, daß man auf den angekündigten Regierungsentwurf (vgl. BT-Drs. VI/1223 S. 4) wartete; vgl. Auernhammer, Kommentar, Einf. RN 16, Gallwas/S/S Einl. RN 23.

11) BT-Drs. VI/3826.

12) BT-Drs. VI/3711.

13) Anlage 1 zu BT-Drs. VI/3826.

und die Vernachlässigung von Datensicherungsmaßnahmen unter Strafe stelle. Außerdem solle der Verstoß gegen Datensicherungsmaßnahmen, "die kein Selbstzweck seien, sondern den Schutz der Information bezweckten", ponälisiert werden und es müsse eine Verschwiegenheitspflicht der Angestellten des Informationssystemes statuiert werden. Die Strafbestimmungen sollten dabei konsequenterweise auch nichtautomatisierte Informationsverarbeitung erfassen. Als Strafrahmen wurde Freiheitsentzug von 1 bis 5 Jahren bzw. eine angemessene Geldstrafe vorgeschlagen [14].

Anfang November 1972 veranstaltete das Bundesinnenministerium daraufhin eine Anhörung und am 25.5.1972 leitete die Bundesregierung dem Bundesrat einen eigenen Entwurf zu, dessen Anwendungsbereich auf personenbezogene Daten in Dateien beschränkt war [15]. Er passierte am 6.7.1973 den Bundesrat. Am 20.9.1973 wurde der Regierungsentwurf mit Stellungnahme des Bundesrates und der Gegenäußerung der Bundesregierung dem 7. Deutschen Bundestag vorgelegt [16]. Nach der ersten Lesung am 29.11.1973 wurde er an den Innenausschuß verwiesen.

Der Bundestag diskutierte zur gleichen Zeit den Regierungsentwurf des Einführungsgesetzes zum Strafgesetzbuch vom 11.5.1973 [17]. Dabei wurden auch die §§ 201 ff. StGB neu geregelt. Als schließlich am 2.3.1974 das Gesetz verabschiedet wurde [18], war mit § 203 n. F. auch "eine erstmalige Regelung von Datenschutzstrafrecht im StGB" [19] erfolgt, was nicht

14) Anlage 1 zu BT-Drs. VI/3826 S. 154.

15) BR-Drs 391/73.

16) BT-Drs. 7/1027.

17) Regierungsentwurf vom 11.5.1973 BT-Drs. 7/550; vgl. dazu auch den 1. Bericht des Sonderausschusses (BT-Drs. 7/1232 und 7/1261).

18) Die Verkündung im BGBl. (S. 469 ff) erfolgte am 9.3.1974.

19) Haft DSWR 1979, 138;, ebenso Arzt/Weber RN 462 und 494 und Ostendorf GA 127 (1980) S.446.

ohne Auswirkungen auf die Strafbestimmungen im Entwurf des Bundesdatenschutzgesetzes (§§ 32, 33 EntwBDSG) blieb [20]. So wurde § 33 EntwBDSG ("Verletzung der Geheimhaltungspflicht") gestrichen, da dieser Tatbestand durch den neugefaßten § 203 II StGB als voll umfaßt angesehen wurde [21]. Die Veränderungen, die § 32 EntwBDSG erfuhr, waren nach der Begründung in den Gesetzesmaterialien nur redaktioneller Natur [22]. So wurde das Merkmal "nicht offenkundig" eingefügt und der Begriff "weitergeben" durch den "umfassenderen Begriff übermitteln" ersetzt [23].

Als der Bundestag nach zweiter und dritter Lesung diesen modifizierten Entwurf am 10.6.1976 annahm [24], waren inzwischen seit der ersten Lesung eines Bundesdatenschutzgesetzes am 29.11.1973 knapp zweieinhalb Jahre vergangen. Der Bundesrat versagte jedoch am 25.6.1976 die Zustimmung zu diesem politisch kontroversen Gesetz und rief den Vermittlungsausschuß an [25]. Bedingt durch den Stimmungsumschwung der Länder Saarland und Niedersachsen [26] fand sich schließlich im Bundesrat eine Mehrheit für das durch die Änderungsvorschläge des Vermittlungsausschusses [27] modifizierte Gesetz. Die Strafbestimmung wurde jedoch inhaltlich nicht geändert, sondern erhielt lediglich eine neue Paragraphennummer: Aus § 32 EntwBDSG wurde § 41 BDSG. Das Bundesdatenschutzgesetz wurde dann am 1.2.1977 im Bundesgesetzblatt verkündet [28].

20) BT-Drs. 7/1027 (21.9.1973).

21) Vgl. die Begründung zur Streichung des § 33 EntwBDSG in BT-Drs. 7/5277 (S. 11) vom 2.6.1976. Wie in der Einleitung dargelegt, soll das Verhältnis zwischen den Strafnormen der Datenschutzgesetze und § 203 StGB ausgeklammert bleiben.

22) BT-Drs. 7/5277 zu § 32 EntwBDSG (S.11).

23) So die Begründung des Innenausschusses zu "seinem" § 2 in BT-Drs. 7/5277 (S. 6).

24) Vgl. BR-Drs. 422/76 vom 11.6.1976.

25) Vgl. BT-Drs. 7/5497 die die Änderungsbegehren des Bundesrates enthält.

26) Simitis in: Simitis/D/M/R Einl. RN 41, schließt "datenschutzfremdes politisches Kalkül" als Grund für die Meinungsänderung nicht aus.

27) BT-Drs. 7/5568.

28) BGBl. I 1977 S. 201

III) Die Lage in den Bundesländern

Auf Landesebene erfolgte die Verabschiedung von Datenschutzgesetzen teils vor dem BDSG, teils erst danach [29].

Das erste Datenschutzgesetz wurde von Hessen Ende 1970 verabschiedet [30]. Es erfaßte "alle für Zwecke der maschinellen Datenverarbeitung erstellten Unterlagen, sowie alle gespeicherten Daten und Ergebnisse ihrer Verarbeitung". Der Geltungsbereich war jedoch auf die öffentliche Verwaltung des Landes Hessen beschränkt [31] und das Gesetz enthielt noch keine Strafbestimmung, sondern nur eine Bußgeldvorschrift [32].

In Rheinland-Pfalz verabschiedete der Landtag am 24.2.1974 ein Landesdatenschutzgesetz [33]. Es war wie das hessische Datenschutzgesetz auf die öffentliche Verwaltung des Landes beschränkt und erhielt in § 1 Abs. 1 LDatG RP eine Definition des Datenschutzes [34]: Danach war Datenschutz "die Vorsorge dafür, daß durch Erfassung, Speicherung, Nutzung und Löschung von Daten schutzwürdige Belange ... nicht beeinträchtigt oder verletzt werden". Ferner wurde eine Strafbestimmung mit folgendem Wortlaut statuiert:

29) Vgl. den Überblick bei Gola MDR 1980, 181.

30) Datenschutzgesetz vom 7.10.1970, GVBl. S. 625.

31) Vgl. § 1 idF vom 7.10.1970, GVBl. S. 625.

32) § 16 idF vom 7.10.1970. Das hessische Datenschutzgesetz wurde am 31.1.1978 dem BDSG angepaßt (was zu einer Verdoppelung der Paragraphenzahl führte) und enthält jetzt in § 32 eine Strafbestimmung, die mit der des BDSG fast wörtlich übereinstimmt.

33) GVBl. 1974 S. 31 f.

34) Es war die einzige Definition dieser Fassung des Gesetzes. Das heutige Datenschutzgesetz vom 31.12.1978 enthält - wie das BDSG - in den ersten drei Paragraphen deren zehn.

§ 15 LDatG Rh-Pf (1974):

(1) Wer dem Datenschutz unterliegende Daten, die ihm im Zusammenhang mit der maschinellen Datenverarbeitung bekannt geworden sind, unbefugt offenbart oder den Zugriff auf solche Daten unbefugt gewährt, wird mit Freiheitsstrafe bis zu einem Jahr und mit Geldstrafe oder mit einer dieser Strafen bestraft.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einem anderen einen Vermögensvorteil zu verschaffen oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren, daneben kann auf Geldstrafe erkannt werden.

(3) Ebenso wird bestraft, wer sich, ohne zu dem in Absatz 1 bezeichneten Personenkreis zu gehören, derartige Daten unbefugt verschafft oder sie unbefugt verwendet.

(4) Die Vorschriften der Absätze 1 bis 3 gelten nur, soweit die Tat nicht in anderen Bestimmungen mit höheren Strafen bedroht sind.

(5) Die Tat wird nur auf Antrag des Verletzten verfolgt. Der Strafantrag kann zurückgenommen werden.

Ende 1978 wurde dieses Landesgesetz dem Bundesdatenschutzgesetz angepaßt [35]. Es enthält jetzt keine Definition des Datenschutzes mehr, sondern in § 1 n. F. eine der Datenverarbeitung, die danach als Speicherung, Übermittlung, Veränderung und Löschung anzusehen ist. In § 1 Abs. 1 a. F. war Datenverarbeitung noch definiert als Erfassung, Speicherung, Nutzung oder Löschung. Nach der jetzigen Definition stellt die Erfassung und Nutzung keine Datenverarbeitung im Sinne des Gesetzes mehr dar, während die Übermittlung und Veränderung nunmehr darunter fallen. Auch die Strafbestimmung wurde grundlegend geändert, sie ist nun der des Bundesdatenschutzgesetzes angenähert. Ein Strafantragsrecht steht nunmehr auch der Datenschutzkommission zu [36].

35) 21.12.1978, GVBl. 1978 S.749.

36) Während zunächst ein Ausschuß für Datenschutz errichtet wurde (§§ 6 ff a. F.), besteht nun - abweichend von allen anderen Bundesländern und dem Bund, die Datenschutzbeauftragte haben - eine Datenschutzkommission (§§ 17 ff. n. F.).

Die übrigen Bundesländer verabschiedeten nach Verkündigung des BDSG eigene Regelungen zum Schutz personenbezogender Daten im Bereich der Landesverwaltung. Das letzte Gesetz in dieser Reihe bildet das Hamburgische Datenschutzgesetz, das am 31.3.1981 verabschiedet wurde [37].

IV) Die Entwicklung nach der Verabschiedung des Bundesdatenschutzgesetzes

Bereits sieben Wochen nach Verabschiedung des BDSG wurde die parlamentarische Diskussion um eine Novellierung eröffnet [38], und Anfang 1980 wurden zwei Gesetzesentwürfe [39] zur Änderung eingebracht, die allerdings beide nicht die erforderlichen Mehrheiten fanden.

Zur Ergänzung des BDSG wurden bereichsspezifische Regelungen geschaffen, wie das Melderechtsrahmengesetz (MRRG) vom 16.8.1980 [40] und das 10. Buch des Sozialgesetzbuches (SGB X) vom 18.8.1980 [41]. Das am 25.3.1982 verkündete Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983) [42] wurde durch das Urteil des BVerfG vom 15.12.1983 für teilweise verfassungswidrig erklärt [43], weshalb ein neues Gesetz geschaffen werden soll.

37) HmbGVBl. S.71. Es trat mit seinen wesentlichen Teilen am 1.5.1981 in Kraft.

38) BT-Drs. 8/191 und 8/266.

39) BT-Drs. 8/3608 (CDU/CSU-Fraktion) und BT-Drs. 8/3703 (SPD u. FDP). Vgl. zu beiden Dehm DSWR 1980, 183 - 185; Meister DuD 1980, 123 - 127 und Wissel/Wronka AfP 3/1980, 134 ff.

40) BGBl. I 1980 S. 1429.

41) BGBl. I 1980 S. 1469.

42) BGBl. I 1982 S. 369. Das Gesetz war am 4.3.1982 vom Bundestag einstimmig verabschiedet worden und die Durchführung durch den am 13.4.1983 verkündeten Beschluß des BVerfG (abgedruckt in JZ 1983, 388) dann ausgesetzt worden.

43) BVerfGE 65, 1 ff. Ebenfalls abgedruckt in der Beilage 56/83 des Bundesanzeigers vom 24.12.1983 (Nr. 241a) und NJW 1984, 419 - 428.

Im Mittelpunkt der weiteren Datenschutzdiskussion stehen die Einführung des neuen, maschinenlesbaren Personalausweises [44], die der sog. "Neuen Medien" [45] und die Novellierung des Bundesdatenschutzgesetzes [46]. Das Urteil des BVerfG übt dabei entscheidenden Einfluß aus. Dies zeigt sich z. B. darin, daß die Einführung der neuen Ausweise verschoben und der Referentenentwurf zur BDSG-Novellierung zurückgezogen wurde [47].

44) BGBl. I 1980 S. 270 und BGBl. I 1983 S. 194 u. 289 f. Die Ausgabe der neuen Ausweise sollte ursprünglich ab dem 1.11.1984 erfolgen.

45) Zu den Rechtsproblemen der sog. "Neuen Medien" vgl. Herb NJW 1983, 2237 f. und die verschiedenen Beiträge in NJW 1984, Heft 8.

46) Vgl. den Referentenentwurf vom 23.6.1983: abgedruckt in DANA 5/83 S. 5 - 10.

47) computer magazin, Heft 6, Juni 1984, S. 6.

B) Die Entwicklung im Ausland

Auch in anderen Staaten wurde erkannt, daß bei der automatisierten Verarbeitung von Daten Gefahren für den Einzelnen und die Gesellschaft drohen. Es sollen deshalb hier kurz die Lösungsversuche anderer Staaten dargestellt werden. Da eine Rechtsvergleichung aller bestehenden Datenschutzgesetze eine eigene Arbeit wert ist, wurde die Betrachtung exemplarisch auf Frankreich, die Schweiz, Österreich, Schweden, Großbritannien und die Vereinigten Staaten von Amerika begrenzt [48] und auf den Vergleich einzelner Gesichtspunkte (vornehmlich der Strafbestimmungen) eingeschränkt. Zu bedenken bleibt allerdings, daß der isolierte Vergleich bestimmter einzelner Gesetze mit denen anderer Rechtsordnungen aufgrund des unterschiedlichen Kontextes stets problematisch ist.

I) Frankreich [49]

Das französische Datenschutzgesetz vom 6.1.1978 über Informatik, Karteien und Freiheiten [50] schützt die Verarbeitung personenbezogender [51] Informationen im öffentlichen und privaten Bereich. Im Gegensatz zum BDSG ist der Schutz insoweit umfassender, als nach Art. 25 bereits die Erhebung von Daten durch

48) Berichte über diese und weitere Staaten finden sich jeweils in den Tätigkeitsberichten des BfD sowie bei Meister RIW/AWD 1982, 481 - 489. Eine synoptische Darstellung des europäischen Datenschutzrechts geben Burkert/Engel DuD 1980, 146 - 152. Zur Zuständigkeit der Europäischen Gemeinschaften auf dem Gebiet des Datenschutzes: Karpenstein S. 889 - 908.

49) Allgemein dazu: Schomerus DuD 1978, 81 - 83; Schindel DSWR 1978, 232 - 235; Bull, 1. TB des BfD (BT-Drs. 8/2460), S. 54 - 55; Ordemann Schomerus Einl. Anm. 3.4; Stadler ÖVD 4/1978, 22 - 23.

50) Loi no 78 - 17 relative à l'informatique, aux fichiers et aux libertés. Kundgemacht am 7.1.1978 im Journal officiel de la République Francaise, S. 227 - 231. Abgedruckt bei Gallwas/S/S IV 7 - 1/ff. Übersetzung von Berhard/Gola/Tuner in DuD 1978, 157 - 162.

51) Art. 4. Der noch im Regierungsentwurf vorgesehene Schutz von Daten über juristische Personen wurde fallengelassen, vgl. dazu Bull, 1. TB des BfD (BT-Drs. 8/2460), S. 54 und Schomerus DuD 1978, 61.

betrügerische, unlautere oder unzulässige Mittel verboten ist [52], während das BDSG erst Regelungen über die Speicherung trifft. Der interessanteste Unterschied zu den deutschen Datenschutzgesetzen liegt darin, daß das französische Gesetz im Art. 2 Aussagen zur Verwertung von Persönlichkeitsprofilen macht. So darf keine richterliche Entscheidung, die eine Bewertung eines menschlichen Verhaltens erhält, auf einer automatischen Datenverarbeitung gründen, die eine Bestimmung des Profils oder der Persönlichkeit des Betroffenen vornimmt [53]. Ferner darf keine Entscheidung einer öffentlichen oder privaten Stelle, die eine Bewertung eines menschlichen Verhaltens enthält, ausschließlich auf einer automatischen Datenverabeitung gründen, die eine Bestimmung des Profils oder der Persönlichkeit des Betroffenen vornimmt [54].

Die in den Art. 41 - 44 niedergelegten Strafbestimmungen sehen Strafen vor zwischen 6 Monaten und 5 Jahren Freiheitsentzug und/oder Geldstrafe von 2 000 bis 2 000 000 FF. So wird nach Art. 41 bestraft, wer den Genehmigungsbeschluß, der gemäß Art. 15 für die Datenverarbeitung öffentlicher Stellen nötig ist, nicht veröffentlicht oder die für nichtöffentliche Stellen erforderliche Anmeldung der Datenverarbeitung unterläßt [55]. Art. 42 sanktioniert die rechtswidrige Datenerhebung, -speicherung und Datensicherungsvorschriften [56]. Darüberhinaus kann das Gericht bei Verstoß

52) Die strafrechtliche Absicherung des Art. 25 erfolgt über Art. 42.

53) Art. 2 Satz 1.

54) Art. 2 Satz 2.

55) Strafe: Gefängnis zw. 6 Mon. und 2 Jahren und Geldstrafe zw. 2 000 und 20 000 FF.

56) Strafe: Gefängnis zw. 1 und 5 Jahren; Geldstrafe zw. 20 000 und 2 000 000 FF.

gegen Art. 41 oder 42 die ganze oder auszugsweise Veröffentlichung des Urteils in einer oder mehreren Zeitungen oder seinen Aushang unter von ihm festzusetzenden Bedingungen auf Kosten des Verurteilten verfügen. Nach Art. 43 wird bestraft, wer durch die Verarbeitung von Daten den Ruf, das Ansehen oder die Privatsphäre verletzt, indem diese Daten unbefugten Personen zur Kenntnis gebracht worden sind. Hierbei ist auch die fahrlässige Begehung strafbar [57]. Durch Art. 44 schließlich wird die Zweckentfremdung von Daten mit bis zu 5 Jahren Freiheitsentzug bedroht [58].

Insgesamt läßt sich sagen, daß der Schutz des Bürgers im französischen Datenschutzgesetz besser und umfassender als in den deutschen Datenschutzgesetzen geregelt ist [59].

II) Schweiz [60]

Auf Bundesebene besteht noch kein Gesetz, jedoch hat der Bundesrat am 16.3.1981 "Richtlinien für die Bearbeitung von Personendaten in der Bundesverwaltung" erlassen und mit Wirkung vom 1.7.1981 in Kraft gesetzt [61]. Diese verwaltungsinternen Weisungen gelten für jede automatisierte und manuelle Bearbeitung von Personendaten (worunter auch Angaben über eine juristische Person fallen).

57) Strafe bei Vorsatz: Gefängnis zw. 2 und 6 Monaten; Geldstrafe zw. 2 000 und 20 000 FF. Bei Fahrlässigkeit: Geldstrafe zw. 2 000 und 20 000 FF.

58) Strafe: Gefängnis zw. 1 und 5 Jahren; Geldstrafe zw. 20 000 und 2 000 000 FF.

59) So wohl auch Schindel DSWR 1978, 232 und 234.

60) Allgemein dazu: Egloff ZSR 96 (1977) I S. 345 - 368; Schweizer DuD 1980, 153 - 156; ders. DuD 1983, 202 - 207 und Ordemann/Schomerus Einl. Anm. 3.

61) Abgedruckt in DuD 1981, 243 - 245. Vgl. dazu auch Schweizer DuD 1980, 153 - 156 und Tuner DANA 2/3/1982, S. 7 - 8.

Im Kanton Genf trat am 1.3.1977 ein Datenschutzgesetz in Kraft (Loi sur la protection des informations traitees automatiqument par ordinateur), das inzwischen revidiert und am 17.12.1981 neu beschlossen wurde. In den anderen Kantonen wurden nur "regierungsrätliche Verordnungen" erlassen, jedoch besteht inzwischen als Vorschlag ein von einem Expertenausschuß erarbeitetes Muster-Datenschutzgesetz für die Kantone [62]. Auch einige Gemeinden haben aus eigener Initiative einen gewissen Datenschutz realisiert. So gibt es z. B. in Lausanne - um nur eine zu nennen - ein Datenschutz-Reglement [63].

Da die Entwicklung in der Schweiz noch nicht abgeschlossen ist, erscheint ein Vergleich mit den deutschen Gesetzen vorläufig wenig sinnvoll.

III) Österreich [64]

Das österreichische Datenschutzgesetz wurde fast zwei Jahre nach dem BDSG, am 18.10.1978, verkündet [65] und ähnelt diesem stark, da auf die Ergebnisse der bundesdeutschen Diskussion zurückgegriffen wurde [66].

Im Unterschied zum BDSG erhält es ein Grundrecht auf Datenschutz [67] und schützt auch Informationen über juristische Personen und handelsrechtliche Personengesellschaften [68].

62) Ein Abdruck des Entwurfs findet sich bei Schweizer DuD 1983, 202 - 207.

63) Eine Aufzählung weiterer Gemeinden bei Schweizer DuD 1980, 155.

64) Allgemein dazu: Pawlikowsky DuD 1978, 22 - 24; Reisinger DuD 1979, 120 - 125 und Stadler ÖVD 11/1978, 8 - 10. Kritisch Wielinger S. 162: "Kompliziertes Vorschriftengestrüpp".

65) Österreichisches BGBl 565/1978.

66) So Reisinger DuD 1979, 120 und Pawlikowsky DuD 1979, 22.

67) Art. 1 § 1. Ob nach dem Volkszählungsurteil des BVerfG (E 65, 1 ff = NJW 1984, 418 ff) auch in der Bundesrepublik ein Grundrecht besteht ("informationelles Selbstbestimmungsrecht") muß bezweifelt werden; jedenfalls aber hat "der Datenschutz" Verfassungsrang.

68) § 3 Ziff. 1.

Das Gesetz, das für den privaten und öffentlichen Bereich gilt, regelt im Gegensatz zu den deutschen Gesetzen bereits die Ermittlung (= Erhebung) von personenbezogenen Daten [69]. Obwohl § 3 eine Reihe von Definitionen enthält, kennt es den Begriff der "Datei" nicht, und für Medienunternehmen findet das Gesetz bis zum Inkrafttreten eines Mediengesetzes nur eingeschränkte Anwendung [70].

Eine auch für das deutsche Recht bedenkenswerte und zu begrüssende Regelung enthält § 47: Danach erhält jede private oder öffentliche Stelle die der Registrierungspflicht unterliegt eine Registernummer. Bei einer Übermittlung muß diese Registernummer angegeben werden. Da dies immer die Nummer der letztübermittelnden Stelle sein muß, kann der Betroffene den Weg der Daten auch bei mehreren Stationen zurückverfolgen und über die Registernummer (das Register ist öffentlich) die datenverarbeitende(n) Stelle(n) erfahren.

Die Strafbestimmungen lauten:

§ 48 Geheimnisbruch

(1) Wer Daten widerrechtlich offenbart oder verwertet, die ihm ausschließlich Kraft seiner berufsmäßigen Beschäftigung mit Aufgaben der Verarbeitung anvertraut worden oder zugänglich geworden sind, und deren Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse des Betroffenen zu verletzten, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

(2) Der Täter ist nur auf Antrag eines in seinem Interesse an der Geheimhaltung Verletzten oder auf Antrag der Datenschutzkommission zu verfolgen.

(3) Die Öffentlichkeit in der Hauptverhandlung ist auszuschließen, wenn dies
1. der Staatsanwalt, der Beschuldigte oder ein Privatbeteiligter beantragt, oder
2. das Gericht zur Wahrung von Interessen am Verfahren nicht beteiligter Personen für notwendig hält.

69) § 6 für den öffentlichen und § 17 für den privaten Bereich. Nach der Legaldefinition in § 3 Ziff. 5 ist die Ermittlung "das Erheben oder sonstige Beschaffen von Daten ohne Rücksicht auf die dabei angewendeten Verfahren".

70) § 54.

§ 49 Unbefugte Eingriffe in Verarbeitungen

Wer widerrechtlich einem anderen in seinen Rechten dadurch absichtlich einen Schaden zufügt, daß er automationsunterstützt verarbeitete Daten löscht, verfälscht oder sonst verändert oder daß er sich automationsunterstützt verarbeitete Daten verschafft, ist, wenn die Tat nicht nach anderen Bestimmungen mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

IV) Schweden [71]

Als Beispiel aus dem skandinavischen Raum ist das schwedische Datenschutzgesetz vom 11. Mai 1973 zu nennen [72], das allerdings nur elektronische Personenregister und nicht - wie die deutschen Gesetze - die manuelle Datenverarbeitung erfaßt. Im Unterschied zum deutschen Recht statuiert das Gesetz eine grundsätzliche Lizenzierungspflicht, in deren Rahmen auch die Beschaffung von Informationen geregelt wird [73]. Ferner unterliegen bestimmte, vom Gesetzgeber als besonders schutzbedürftig angesehene Daten (z. B. über Straftaten, Zwangsmaßnahmen, Krankheiten, soziale Hilfen, politische oder religiöse Anschauungen) einer beschränkten Verarbeitung (teilweise nur durch öffentliche Stellen) [74]. Die beiden Strafbestimmungen [75] sehen Strafen bis zu einem bzw. bis zu zwei Jahren Freiheitsstrafe vor, wobei eine Strafverfolgung zum Teil nur auf Antrag der geschädigten Person oder bei Vorliegen eines öffentlichen Interesses möglich ist. Neben dem Datenschutzgesetz existiert in Schweden

71) Allgemein dazu: Mallmann ÖVD 1974, 31 - 33 und Hellner S. 265 - 283.

72) Datalagen (SFS 1973: 289); Übersetzung in ÖVD 1974, 240 - 243 und bei: Simitis/D/M/R, Dokumentation, D 9.1.

73) § 2. Die ursprüngliche strenge Lizenzierung wurde durch eine Novellierung vom 1.7.1979 vereinfacht.

74) § 4.

75) §§ 20, 21.

seit dem 1. Juli 1974 ein Gesetz über das Kreditauskunftswesen [76]. Ferner ist der Adressenhandel erheblich eingeschränkt, da ab dem 1. Juli 1981 Gesamtverzeichnisse von Anschriften nur noch durch staatliche Stellen aufgelegt werden dürfen [77].

Insgesamt läßt sich sagen, daß das schwedische Datenschutzgesetz stärker am Schutz des Bürgers ausgerichtet ist.

V) Vereinigte Staaten von Amerika [78]

Die Gesetzgebungskompetenz ist in den Vereinigten Staaten stärker aufgesplittert und die Regelungstechnik im allgemeinen sehr viel kasuistischer als in den kontinental-europäischen Ländern. Doch nicht nur die unterschiedliche Rechts- und Verfassungstradition, sondern auch die andersartigen Strukturen von Wirtschaft und Verwaltung sind zu bedenken. Ein einheitliches und übergreifendes Datenschutzgesetz gibt es nicht, sondern die Gesetzgeber im Bund und in den einzelnen Staaten versuchen, die spezifischen Gefahren durch bereichsorientierte Gesetze abzuwenden. Hier sind insbesondere [79] bedeutsam:

Der "Privacy Act" vom 31.12.1974 [80], der den Schutz des Persönlichkeitsrechtes vor Mißbrauch von Daten bezweckt. Er gilt nur für Behörden und Ämter des Bundes, unabhängig davon, ob

76) Kredituppplysningslagen 1973: 1173.

77) Vgl. dazu Bull, 1. TB des BfD (BT-Drs. 8/2460), S. 73 und Sieglerschmidt S. 234.

78) Allgemein dazu: Bull, 2. TB des BfD (= BT-Drs. 8/3570), S. 71 - 72; Somerus ÖVD 11/1977, 3 - 7; Ordemann/Schomerus Einf. 3.1. und Simitis in: Simitis/D/M/R, Einl. RN 70.

79) Eine Aufzählung weiterer Gesetze bei Simitis in: Simitis/D/M/R, Einl. RN 70. Zu Gesetzesinitiativen: Schomerus/Neumann DVR 1981, 239 ff.

80) Public Law 93-579 93. US-Congress S. 3418. Übersetzung von Schindel, Das amerik. Datenschutzgesetz; sowie bei Simitis/D/M/R, Dokumentation, D 8.1. Vgl. weiter dazu Stadler ÖVD 1/2/1977, 17 - 18 und von Groeben ÖVD 5/1977, 17 - 18.

automatisiert oder manuell personenbezogene Informationen verarbeitet werden. Die Strafbestimmung sieht vor, daß jeder bestraft wird, der aufgrund falscher Angaben von einer Behörde personenbezogene Daten eines anderen verlangt oder sich beschafft. Beamte oder Angestellte einer Behörde können bestraft werden, wenn sie aufgrund ihrer Beschäftigung bei einer Behörde erlangte individuell identifizierbare Informationen weitergeben oder gegen eine im Gesetz niedergelegte Bekanntmachungspflicht über Bestehen oder Charakter einer Datenbank verstossen. Alle diese Strafbestimmungen sehen Geldstrafe bis zu 5 000 Dollar vor. Verschiedene Staaten haben für ihre Verwaltung ähnliche "Privacy Acts" (oder "Fair Information Practices Acts") erlassen.

Der ebenfalls auf Bundesebene gültige "Fair Credit Reporting Act" [81] trat am 25.4.1971 in Kraft und trifft Bestimmungen über die Arbeit der Auskunfteien, gleichgültig, ob sie mit Computern oder herkömmlichen Mitteln arbeiten. Dabei sind die Auskunfteien grundsätzlich verpflichtet, dem Betroffenen ihre Informanten mitzuteilen und die Weitergabe von Daten, die ein länger als 7 (bzw. 14) Jahre zurückliegendes Ereignis beschreiben ist nicht erlaubt.

Schließlich existiert noch der vom Bund erlassene "Fair Credit Billing Act" [82], der den Bürger von Nachteilen aus Fehlern bei der Abwicklung von Geschäften mittels Kreditkarten schützen will.

81) Fair Credit Reporting Act vom 26.10.1970 Public Law 91 - 508. Vgl. hierzu: Mallmann RIW/AWD 1973, 78 - 84.

82) Vgl. dazu den 2. TB des BfD (= BT-Drs. 8/3570) S. 71.

VI) Großbritannien [83]

Bereits 1972 legte eine unabhängige Studienkommission, das Committee on Privacy, der Regierung einen Bericht vor [84] und im Januar 1979 wurde der Bericht eines als Nachfolger arbeitenden Komitees vorgestellt [85]. In diesem über 400 Seiten starken "Report of the Committee on Data Protection" wird vorgeschlagen, durch Gesetz die Grundsätze der personenbezogenen Datenverarbeitung festzulegen und eine "Data Protction Authority" einzusetzen, die Regeln ("codes of Practice") aufstellen soll, die sich auf einzelne Anwender, Gruppen von Anwendern, einzelne Systeme oder Gruppen von Systemen beziehen. Es werden ca. 50 Bereiche und Anwendergruppen aufgezählt, darunter die Presse und Textverarbeitungssysteme [86]. Da keine der Vorschläge bisher umgesetzt wurden, besteht bis heute in Großbritannien kein Datenschutzgesetz. Die Regierung will jedoch dem Parlament einen Entwurf vorlegen, der sich aber auf die Festlegung allgemeiner Datenschutzgrundsätze beschränken soll und keine unabhängige Datenschutz-Kontrollinstanz schafft [87].

83) Allgemein dazu: Burkert DuD 1979, 126 - 130; Bull, 1. TB des BfD (= BT-Drs. 8/2460) S. 61; Ordemann/Schomerus Einl. 3.7 und Stadler ÖVD 5/1979 S. 11 - 12.

84) Home Office, Committee von Privacy, Chairman: Sir Kenneth Younger, London, July 1972, Cmnd. 5012.

85) Home Office, Report of the Committee on Data Protection, Chairman: Sir Norman Lindop, London, December 1978, Cmnd.7341 (sog. "Lindop-Report").

86) Anhang 9 des Lindop-Reports (S. 409 - 410).

87) 4. TB des BfD, S. 60.

§ 3

Die Verweisungstechnik der Datenschutzgesetze

Viele in den letzten Jahren entstandenen Gesetze sind geprägt von großzügigen Verweisungen, die in Literatur und Rechtsprechung als besondere Form der Gesetzgebungstechnik angesehen werden [1]. Verweisungen sollen nicht nur den Gesetzgeber entlasten, indem sie Wiederholungen vermeiden und den Gesetzeswortlaut straffen, sondern auch die Systematik der Rechtsordnung bzw. des Gesetzes deutlicher werden lassen und damit zur Rechtsvereinheitlichung beitragen [2]. Es besteht aber andererseits die Gefahr, daß damit die Überschaubarkeit und Anschaulichkeit der Regelung verloren gehen kann [3], weshalb Verweisungen auch als "grobe Unhöflichkeit" [4] des Gesetzgebers bzw. "verwerfliche Art der Gesetzesgestaltung" [5] kritisiert werden. In § 35 der ministeriellen Richtlinien des Bundes zur Gesetzestechnik [6] heißt es:

"Gesetze müssen sprachlich einwandfrei und soweit möglich für jedermann verständlich gefaßt sein.

Verweisungen sind möglichst zu meiden; insbesondere sollen Verweisungen auf Vorschriften unterbleiben, die ihrerseits wiederum auf andere Vorschriften verweisen. Wenn sie vorkommen, sollen sie so gefaßt werden, daß der Leser den Grundgedanken der Vorschrift ohne nachzuschlagen versteht."

1) Aus der Rechtsprechung statt aller: BVerfGE 47, 285, 311. Aus der Literatur: Hill S. 114; Karpen S. 4; Kindermann S. 71, Maurer GewArch 1982, 13; Ossenbühl DVBl 1967, 401; Noll S. 227 ff.

2) Hill S. 114, Karpen S. 11.

3) Karpen S. 10 sowie S. 222; Kindermann S. 47.

4) Hugger S. 301; Staats ZRP 1978, 60.

5) Dölle S. 43 kritisierte schon 1949 eine fünfgliederige Verweisungskette als "verwerfliche Art der Gesetzesgestaltung".

6) "Gemeinsame Geschäftsordnung der Bundesministerien - Besonderer Teil (GGO II)" vom 1.8.1958 in der Fassung der Neubekanntmachung vom 15.10.1976 durch den Bundesminister des Inntern GMBl. 1976 S. 550 - 568 (S. 557).

Untersucht sein soll, inwieweit übermäßige Verweisungen zu Fehlern in der Rechtsanwendung führen. Dazu soll zunächst die Verweisungstechnik im allgemeinen und in bezug auf das BDSG im speziellen dargestellt und näher analysiert werden. Ausgeklammert bleibt der bei § 41 BDSG bestehende Streit, ob die Strafbestimmung wegen der Unbestimmtheit des Merkmals "unbefugt" verfassungswidrig ist, bzw. ob die exzessive Verwendung von Generalklauseln zur Verfassungswidrigkeit führt [7], da die Fragen, die sich, gerade im Strafrecht, aus der Unbestimmtheit von einzelnen Begriffen ergeben, alte und häufig erörterte Probleme der juristischen Dogmatik sind [8].

Im Abschnitt A des Kapitels erfolgt nach einer Einführung eine Klassifizierung der Verweisungen und die Darstellung ihrer Problematik einschließlich der Erörterung einer "absoluten Grenze" der Verständlichkeit von Verweisungen.

7) Nach Arzt/Weber RN 523, verstößt § 41 BDSG gegen Art. 103 II GG; Schünemann, nulla poena sine lege?, spricht auf S. 7 von einer "flagranten Verletzung des Bestimmtheitsgrundsatzes" und hält auf S. 37 § 41 wegen der Generalklauseln für verfassungswidrig; ders. bei Berz ZStW 90 (1978) S. 216. Fiedler DuD 1980, 77 äußert "aktuelle Zweifel an der verfassungsmäßigen Bestimmtheit des § 41 BDSG"; Tubies DuD 1981, 152", kritisch auch Kamlah: in Burhenne /Perband § 41 RN 7; Tiedemann NJW 1981, 946: "legt geradezu die Annahme eines Verfassungsverstoßes nahe"; ders. JZ 1982, 520 (strafrechtl. Generalklausel (§ 41 BDSG) verfassungswidrig); ders. bei Berz ZStW 90 (1978) S. 216; kritisch auch von Uckermann DuD 1978, 67. Zu § 32 EntwBDSG, der § 41 BDSG fast entspricht, Zielinski S. 147. Zur Kritik an der "gehäuften Verwendung von Generalklauseln bzw. Leerformeln" im BDSG ferner: Sasse, Das BDSG, S. 81; Becker Schleswig-Holsteinische Anzeigen 1980, S. 26; Marx DSWR 1979, 86; Simitis NJW 1981, 1698; Kamlah, DVD-Tagung 1982, S. 63. Andererseits muß auch gesehen werden, daß ohne die Verwendung allgemeiner Begriffe - auch im Strafrecht - der Gesetzgeber nicht in der Lage wäre, der "Vielgestaltigkeit des Lebens Herr zu werden": BVerfGE 4, 352, 358; 11, 234, 237, Nach Naucke (1973) ist das Nebenstrafrecht ohne Generalklauseln kaum vorstellbar und nach Schulz BKK 1978, 57 machen gerade die Generalklauseln das BDSG interpretationsfähig.

8) Vgl. für das Strafrecht nur die Nachweise bei Maunz/Dürig/Herzog Art. 103 RN 107 und speziell zum Nebenstrafrecht: Tiedemann, Tatbestandsfunktionen.

Abschnitt B befaßt sich mit den von § 41 BDSG ausgehenden Verweisungen. Dieses komplexe System wird dabei sprachlich und mit Hilfe von Abbildungen und Graphiken dargestellt und analysiert werden.

Schließlich wird in einem Exkurs (Abschnitt C) die Strafbestimmung eines bereichsspezifischen Gesetzes (§ 79 SGB X), die auf § 41 BDSG verweist, erläutert.

A) Die Verweisungstechnik

Bevor die Problematik von Verweisungen näher dargestellt und erläutert wird, soll ein Überblick über die heute anerkannte Klassifizierung von Verweisungen gegeben und die des BDSG darin eingeordnet werden.

I) Die Klassifizierung von Verweisungen

Die Einteilung nach einzelnen Verweisungstypen ist nicht immer ganz einheitlich, da in der Literatur verschiedene Verweisungsklassifizierungen gebildet wurden und sie sich teilweise überschneiden [9]. Dennoch läßt sich cum grano salis eine herrschende Meinung bei der Gliederung von Verweisungstypen ausmachen. Von dieser "Formenlehre der Verweisung" [10] soll im folgenden ausgegangen werden, da die Bildung neuer, eigener Strukturen für das Problem der Verweisungskomplexität keinen Fortschritt brächte.

9) Zur Einteilung von Verweisungen, die nach A. Schnell, Diss. Tüb. 1984, "botanischen Bestimmungsbüchern" ähneln, vgl. nur die ausführlichen Werke von Berger und Karpen.

10) Kindermann S. 71.

In der vorliegenden Arbeit soll besonders Berger [11] und Karpen [12] gefolgt und drei ihrer Einteilungskriterien vorgestellt und die Verweisungen der Datenschutzgesetze darin eingeordnet werden: Dies ist zum einen die Trennung von Binnen- und Außenverweisungen, zum anderen die von dynamischen und statischen Verweisungen und schließlich von expliziten (ausdrücklichen) und impliziten (stillschweigenden) Verweisungen. Daneben gibt es weitere Einteilungsmodalitäten [13], die jedoch als für die Arbeit unergiebig ausgeschieden wurden.

1) Zunächst einmal lassen sich Binnen- und Außenverweisungen unterscheiden [14].

Binnenverweise sind Verweise auf Vorschriften desselben Gesetzes (oder seiner Anlagen), während Außenverweise eine Bezugnahme auf andere Normen darstellen. Im BDSG kommen beide Arten vor: Während die Begriffsdefinitionen und die Verweise auf andere Paragraphen Binnenverweise sind, ist die Subsidiaritätsregelung des § 7 II BDSG mit seinem Verweis auf die Landesdatenschutzgesetze, sowie die Subsidiaritätsklausel des § 45 BDSG eine Außenverweisung.

2) Die zweite Einteilung gliedert danach, ob die Verweisungen dynamisch oder statisch sind [15].

11) Berger, Die Erschließung von Verweisungen bei der Gesetzesdokumentation, München-Pullach 1971.

12) Karpen, Die Verweisung als Mittel der Gesetzgebungstechnik, Berlin 1970.

13) Das juristische Informationssystem des Bundes (JURIS) unterscheidet etwa 50 unterschiedliche Verweisungsarten: Hugger S. 304.

14) Berger S. 169; Karpen S. 12 f.; Kindermann S. 73; Krey, EWR 2/81, S. 127.

15) Berger S. 171; Karpen S. 67; Kindermann S. 73; ders. in: Öhlinger, Methodik der Gesetzgebung, S. 230; Krey EWR 2/81 S. 128. Auch das BVerfG nimmt diese Unterscheidung vor: BVerfGE 47, 285, 310 ff. = NJW 1978, 1475 ff.

Dynamisch sind Verweisungen, wenn sie auf die jeweils geltende Fassung anderer Normenkomplexe, statisch, wenn sie nur auf die zum Zeitpunkt des Erlasses des verweisenden Gesetzes geltende Fassung des anderen Normenkomplexes verweisen. § 7 II BDSG wird man wohl als dynamische Verweisung auffassen müssen, so daß die jeweils geltenden Landesgesetze insoweit dem BDSG vorgehen [16].

3) Als letztes lassen sich explizite (ausdrückliche) und implizite (stillschweigende) Verweisungen unterscheiden [17].

Bei einer expliziten Verweisung wird die Norm, auf die weiter verwiesen wird, expressis verbis genannt. So ist z. B. § 1 II BDSG, der ausdrücklich die §§ 7, 22, 31 BDSG aufführt und bezeichnet, eine explizite Verweisung; ebenso der von Wochner [18] als "rechtstechnisch verunglückte Regelung" angesehene § 7 I 1 BDSG. Als implizite Verweisungen werden solche bezeichnet, bei denen sie sich stillschweigend aus Systematik bzw. Sinn und Zweck ergeben. So ist die in § 41 BDSG gebrauchte Formulierung "... die dieses Gesetz schützt ..." eine stillschweigende Verweisung auf § 1 II BDSG, in dem es heißt: "Dieses Gesetz schützt ...". Aber auch auf die vielen Legaldefinitionen [19] in § 2 BDSG wird implizit verwiesen.

16) Nach dem BVerfG ist es unter rechtsstaatlichen und demokratischen Gesichtspunkten problematisch, auf dynamische landesrechtliche Normen zu verweisen: NJW 1978, 1475 mit Anm. von Baden NJW 1979, 623 - 626, der (auch) einen Überblick über die Gesamtproblematik gibt.

17) Karpen S. 33 unterscheidet ausdrückliche und stillschweigende Verweisungen; ebenso Noll S. 228. Berger S. 15 unterteilt in voll-explizite, halb-explizite, implizite und stillschweigende Verweisungen.

18) Wochner DVBl 1982, 235.

19) Brinckmann, ÖVD 1972, 63, hält Legaldefinitionen für grundsätzlich unbefriedigend, weil damit keine Klarheit über die Bedeutung des definierten Wortes geschaffen werde; dies geschehe besser durch Explikation, so durch beispielhafte Aufzählung der unter einen Begriff fallenden Unterklassen. Vgl. auch Noll, JZ 1963, 298 f. Zur generellen Problematik juristischer Definitionen: Klug in: Gedächtnisschrift für Rödig S. 199 ff.; ders. Jurist. Logik, 4. Aufl. S. 88 ff.

Diese Einteilung verdeutlicht zunächst nur die Gliederungsmöglichkeiten und Arten von Verweisungen, sagt jedoch nichts über Anzahl und Verhältnis der Verweisungsnormen zueinander aus.

II) Die Problematik von Verweisungen

Wie alle Gesetze, die sich durch eine intensive Verweisungstechnik auszeichnen, werden auch die Datenschutzgesetze kritisiert [20]. So wird das Zusammenspiel der Normen der Datenschutzgesetze in Bezug auf Inhalt und Form beanstandet: Wochner spricht von einem "Datenschutzdurcheinander" und "übertriebener Kompliziertheit" [21] und Schneider und Steinbrinck werfen dem BDSG vor, es kenne "offensichtlich mindestens zwei Sprachebenen" [22]. Das BDSG wird von Laduga als "lex imperfecta" bezeichnet [23] und Müller-Lutz beklagt, daß es "auch für den Fachmann nicht voll überschaubar" sei und "erhebliche Rechtsunsicherheit" schaffe [24]. Schließlich wird die von Marx kritisierte "vielgliedrige Verweisungskette" [25] von Dammann sogar als Grund für "datenschutzrechtliche Unglücksfälle" angesehen [26]. In der Praxis scheitern sogar Landgerichte "glorreich" [27] am Problem der "extrem komplizierten" Verweisungstechnik des BDSG [28], die einen "kaum durchdringlichen Verweisungsdschungel geschaffen hat" [29].

20) Arzt, S. 134, hat schon 1977 festgestellt, daß das Problem des BDSG in den Verweisungen steckt. Kritisch auch Ringwald, INPOL und StA, § 2 III 1 (S. 56).

21) Wochner DVBl 1982, 233 u. 239.

22) Schneider/Steinbrinck online-adl 1979, 478. Zur Sprache der Datenverarbeiter und Datenschützer: Ruckriegel ÖVD 1981, 3 ff.

23) Laduga DuD 1978, 204.

24) Müller-Lutz VW 1976, 907 u. 908.

25) Marx DSWR 1978, 87.

26) Dammann NJW 1978, 1906.

27) Haft NJW 1979, 1196.

28) Riemer S. 32 bei Becker, Schleswig-Hollsteinische Anzeigen S. 25 - 33.

29) Hümmerich/Kniffka NJW 1979, 1189.

Diese vielschichtige Kritik an den Datenschutzgesetzen weist zugleich auf die zwei Hauptprobleme der Verweisungstechnik hin:

1) Zum einen steigt mit zunehmender Komplexität die Gefahr von Fehlern in der Rechtsanwendung. Aufgrund der in den nachfolgenden Kapiteln dargestellten Ergebnisse der empirischen Auswertung kann nur dem zugestimmt werden, was der Ausschuß für Datenschutz des Landes Rheinland-Pfalz bereits Ende 1978 feststellte [30]:

"Angesichts des außerordentlich komplizierten Aufbaues des Bundesdatenschutzgesetzes und des verwirrenden Nebeneinander von Bundes- und Landesrecht kann es nicht verwundern, daß gelegentlich auch fehlerhafte Entscheidungen zustande kommen."

2) Auf der anderen Seite kann die Komplexität von Verweisungen nicht nur zu einer falschen Rechtsanwendung führen, sondern auch zur Verfassungswidrigkeit eines Gesetzes [31].

Die abschließende Beantwortung der Frage, inwieweit komplizierte Verweisungen verfassungswidrig sein können, kann hier nicht erfolgen [32]. Hingewiesen werden muß jedoch darauf, daß bei einer übermäßigen Verweisungstechnik insbesondere ein Verstoß gegen die Gebote der Normenklarheit [33] und Bestimmtheit [34] in Betracht kommt.

30) LT-Drs. 8/3492 S. 5.

31) Ausführlich dazu A. Schnell, Dissertation Tübingen 1984; ansatzweise Ausführungen in BVerfGE 5, 25, 33; 8, 274, 302; BayVGHE Bd. 67 (Bd. 4 n. F) S. 90, 103, 106 und bei Tiedemann NJW 1980, 1559.

32) Hierzu muß auf die erwähnte Arbeit von A. Schnell, Diss. Tüb. 1984, verwiesen werden.

33) Zum Gebot der Normenklarkeit: BVerfGE 27, 1, 8 mwN; 31, 255, 264; 45, 400, 420; 62, 169, 183; BayVerfGH in BayVGHE Bd. 67 (Bd. 4 n. F.) S 90, 103, 106; BVerfG NJW 1984, 422 u. 424. Aus der Literatur statt aller: Maunz/Dürig/Herzog, Art. 20, VII. RN 63 (S. 284).

34) Für das Strafrecht gilt insbesondere Art. 103 II GG; dazu statt aller: Maunz/Dürig/Herzog, Art. 103 II RN 106 ff. Ausführlich zum Problem Verweisungen und Bestimmtheitsgrundsatz: A. Schnell, Diss. Tüb. 1984.

Das Gebot der Normenklarheit wird vom BVerfG aus dem Rechtsstaatsprinzip abgeleitet und nur dann als gewahrt angesehen, wenn sich Voraussetzungen und Umfang von Regelungen "klar und für den Bürger erkennbar ergeben" [35]. Für das BVerfG ist entscheidend, ob "dem Rechtsunterworfenen ohne Zuhilfenahme spezieller Kenntnisse, die wohl bei den mit der Sache befaßten Behörden und Gerichten, nicht aber beim Rechtsunterworfenen vorausgesetzt werden können, ... die Ermittlung dessen, was Rechtens sein soll" möglich ist [36]. Aus dem Rechtsstaatsprinzip folge, daß alle Gesetze den Geboten der Normenklarheit und Bestimmtheit entsprechen müssen. Bei Strafnormen jedoch müssen, wie Art. 103 II GG zeigt, "hinsichtlich der Bestimmtheit besonders strenge Anforderungen gestellt werden" [37]. Auch nach der Literatur ist im Strafrecht die Allgemeinverständlichkeit eines Gesetzes besonders notwendig [38].

Eine übermäßige Komplexität von Verweisungen kann somit die Gebote der rechtsstaatlichen Normenklarheit und strafrechtlichen Bestimmtheit verletzen. Die Grenze,ab der Verweisungen stets verfassungswidrig sind, ist jedenfalls dann erreicht, wenn die Komplexität einen derartigen Umfang erreicht hat, daß ein Verständnis der Zusammenhänge und des zugrundeliegenden Systems aus psycho-biologischen Gründen unmöglich ist ("absolute Verständnisgrenze") [39].

35) BVerfG NJW 1984, 418, 422 mwN.

36) BVerfGE 5, 25, 33.

37) BayVerfGH in BayVGHE Bd. 67 (= Bd. 4 n. F.) S. 90, 106.

38) Baumann, AT § 13 I. 3 (S. 154); ders. MDR 1958, 396; Kindermann S. 34; Tiedemann NJW 1980, 1559; ders. Tatbestandsfunktionen S. 197 f. und 242 (jeweils mwN); Lenckner JuS 1968, 305; Deubner NJW 1969, 623. Nach Noll, Die Berücksichtigung der Effektivität, S. 144, sind "einfache und bestimmte Normen leichter zu sanktionieren als komplizierte und unbestimmte".

39) Dazu sogleich die nachfolgenden Ausführungen, sowie A. Schnell, Diss. Tü. 1984.

III) Die psycho-biologische Verständnisgrenze

Verweisungen sind verfassungswidrig, wenn es niemanden mehr möglich ist, sie zu verstehen, also die absolute Verständnisgrenze erreicht ist [40]. Die Leistungsfähigkeit eines menschlichen Gehirns ist nicht nur von den verschiedensten Faktoren (z. B. Müdigkeit, Alter etc.) abhängig, sondern kann auch individuell differieren. Unabhängig davon gibt es jedoch eine psycho-biologisch bedingte absolute Grenze, ab der der Text und Sinngehalt einer Norm bzw. einer Normenkette nicht mehr verarbeitet werden kann [41].

1) Wahrnehmungspsychologische Grundlagen

Da das Verstehen eines längeren Satzes von der Merkfähigkeit des menschlichen Gehirns abhängt [42], soll hier kurz ein vereinfachtes wahrnehmungspsychologisches Modell zur Informationsaufnahme und -verarbeitung beim Menschen in einer Abbildung vorgestellt und erläutert werden [43]:

Abb. 3.1 "Informationsverarbeitung":

40) A. Schnell, 2. Kap. § 3 V, die von der "psycho-biologischen Grenze der Tatbestandsumschreibung" spricht.

41) A. Schnell, 2. Kap. § 3 V; ansatzweise auch Haft, Einführung in das juristische Lernen, der dort auf S. 14 von "Kapazitätsbeschränkungen des Simultangedächtnisses" spricht.

42) Weltner, Informationstheorie, S. 128; Dorsch, Psychologisches Wörterbuch, Stichwort "Gedächtnis"; Frank, Kybernetische Grundlagen, Bd. 2, S. 72.

43) Dieses Modell stammt im wesentlichen von Helmar Frank. Es ist in umfassender Form abgedruckt bei Frank, Informationspsychologie, S. 213; ders. Kybernetische Grundlagen, Bd. 2 S. 67. Die hier dargestellte vereinfachte Abbildung und die nachfolgenden Erläuterungen finden sich bei Weltner, Informationstheorie, S. 110 f.; eine ausführliche Beschreibung dieses informationspsychologischen Modells bei Frank, Kybernetische Grundlagen, Bd. 2 S. 64 ff.

44) Die kleinste Einheit zur Darstellung binär verschlüsselter Daten wird bit (von engl. binary digit) genannt.

Aus seiner Umwelt empfängt der Mensch über die verschiedenen peripheren Organe (Sinnesorgane, Rezeptoren), mithin über unterschiedliche Wahrnehmungskanäle, optische, akustische, taktile Informationen, aber auch Geruchs- und Geschmacksinformationen. Der auf die Sinnesorgane auftreffende Informationsfluß ist außerordentlich groß, er liegt für die optischen Rezeptoren (Augen) bei 10^6 bit pro Sekunde, für die akustischen Rezeptoren bei 10^4 pro Sekunde, während er für andere Rezeptoren erheblich darunter liegt [45]. Die wahrgenommene (perzipierte) Information wird codiert und durch Neuronennetzwerke und -leitungen abgeleitet. Dabei tritt eine Reduzierung der Information um mehrere Größenordnungen ein, denn der bewußt wahrgenommene - apperzierte - Informationsfluß liegt in der Größenordnung von ungefähr 16 bit pro Sekunde [46]. Diese Information gelangt zunächst in den Kurzspeicher [47]. Da die Kapazität des Kurzspeichers beschränkt ist, werden pro Sekunde nicht nur 16 bit gespeichert, sondern es gehen gleichzeitig (andere) 16 bit pro Sekunde verloren [48].

45) Weltner, Informationstheorie, S. 110; Frank, Informationspsychologie, S. 71, geht von einem peripheren Reizzustrom von max. 10 bit/sec. aus.

46) Frank, Informationspsychologie, S. 206. Er stellt allerdings selbst fest, daß die Untersuchungen zwischen 10 und 25 bit/sec. streuen. Nach Weltner, Informationstheorie, S. 112 und Gunzenhäuser, S. 226, schwankt die bewußte Aufnahmekapazität von 10 bis 20 bit/sec.; (alle drei jeweils mwN).

47) Weltner, Informationstheorie, S. 113; Dorsch, Psychologisches Wörterbuch, S. 208, 238; Vester S. 59.

48) Dorsch, Psychologisches Wörterbuch, Stichwort "Kurzzeitspeicher"; Frank, Informationspsychologie, S. 207; Weltner, Informationstheorie, S. 113.

Das (altersabhängige) Fassungsvermögen liegt bei Erwachsenen bei ca. 160 bit [49]. Als "Enge des Bewußtseins" ist diese Tatsache, wenngleich nicht in dieser quantitativen Zuschärfung, in der Psychologie beschrieben [50].

Der Kurzspeicher beschreibt in diesem Modell also das Bewußtsein und hat zwei Eigenschaften [51]:

1. Er nimmt Informationen über die Sinnesorgane aus der Umwelt auf, doch ist der Informationsfluß begrenzt. Zusätzlich kann Information aus einem anderen Speicher, dem Gedächtnis, in das Bewußtsein gelangen.

2. Die Information kann für begrenzte Zeit, die Gegenwartsdauer, vollständig im Bewußtsein erhalten bleiben. Innerhalb der Gegenwartsdauer findet die Verarbeitung der als Bewußtseinsinhalte vorliegenden Information statt.

Ein Teil der Information, die im Bewußtsein war, kann danach in einem anderen Informationsspeicher, dem Gedächtnis, gespeichert werden. Das gilt auch für jene Information, die weder der Wahrnehmung, noch dem Gedächtnis entstammt, sondern das Ergebnis informationsverarbeitender Prozesse im Kurzspeicher ist [52].

49) Dorsch, Psychologisches Wörterbuch, Stichwort "Kurzzeitspeicher". Nach Weltner, Informationstheorie, S. 113, liegt die Kapazität beim Erwachsenen zwischen 100 und 200 bits. Nach Frank, Informationspsychologie, S. 207 höchstens bei 160 bits; ders., Kybernetische Grundlagen, Bd. 2 S. 86. Schließlich gibt Gunzenhäuser, S. 226, die Kapazität mit 100 bis 200 bits an.

50) So Frank, Informationspsychologie, S. 207; ders., Kybernetische Grundlagen Bd. 2 S. 86; Weltner, Informationstheorie, S. 113; Riedel GrKG 1967, Bd. 8 S. 1 bezeichnet den Kurzspeicher als "Ort der Gegenwärtigung".

51) Zitiert nach Weltner, Informationstheorie, S. 111 und Frank, Kybernetische Grundlagen Bd. 2 S. 66.

52) Weltner, Informationstheorie, S. 111; Frank, Kybernetische Grundlagen Bd. 2 S. 66 f.

Beim Gedächtnis wird zwischen dem Kurz- und Langgedächtnis unterschieden [53]. Für eine grobe Unterscheidung genügt es, ein Kurzgedächtnis - für Stunden und Tage - und ein Langgedächtnis - für Monate und Jahre - anzunehmen. Die in das Gedächtnis eingespeicherte Information kann in das Bewußtsein zurückgerufen werden. Im Laufe der Zeit zerfällt die eingespeicherte Information, sie wird vergessen [54]. Die Zuflußkapazität ins Kurzgedächtnis beträgt zwischen 0,5 und 1 bit/sec., die ins Langgedächtnis 0,05 bis 0,2 bit/sec. [55].

Ein Satz kann nur dann verstanden werden, wenn alle Elemente im Kurzspeicher vergegenwärtigt werden können [56]. Enthält er mehr als 160 bit Information, wird er nicht schon durch einmaliges Lesen, sondern erst durch mehrmaliges Lesen, Interpretation und Analyse verstanden [57].

Der Informationsgehalt eines Wortes (in bit) ist abhängig von dessen Länge und Bedeutung. Er schwankt in der Regel zwischen 5 und 15 bits [58]. Als mittlere Information eines Wortes der deutschen Sprache nimmt Frank ungefähr 10,9 bit an [59].

53) Das Kurzgedächtnis darf nicht mit dem Kurzspeicher verwechselt werden!

54) Weltner, Informationstheorie, S. 111.

55) Weltner, Informationstheorie, S. 114. Es gibt dazu verschiedene Auffassungen, jedoch sollen die Zahlen hier nur die Größenordnungen verdeutlichen. Nach Riedel, GrKG 1967 Bd. 8 S. 21, beträgt sie beim Langzeitgedächtnis 0,1 bit/sec.

56) Dorsch, Psychologisches Wörterbuch, Stichwort "Gedächtnis"; Weltner, Informationstheorie, S. 128; Frank, Kybernetische Grundlagen, Bd. 2,S.72.

57) Weltner, Informationstheorie, S. 128.

58) Weltner S. 38 f. Frank, Informationspsychologie, S. 189 nimmt zwischen 1 und 5 bit pro Laut an.

59) Frank, Kybernetische Grundlagen, Bd. 1, S. 202.

Der Kurzspeicher ist jedoch nicht nur hinsichtlich der Informationsmenge (160 bit) beschränkt, sondern zusätzlich durch die Anzahl der gleichzeitig zu vergegenwärtigenden Elemente begrenzt. So können nur etwa 7 verschiedene Elemente gleichzeitig bewußt gemacht werden [60].

Diese kurzen Ausführungen sollen verdeutlichen, daß es eine psycho-biologische Grenze gibt, ab der niemand mehr in der Lage ist, einen Text zu verstehen. Wo diese Grenze exakt verläuft, ist letztlich von kompetenterer medizinischer Seite darzulegen. Hier soll nur darauf aufmerksam gemacht werden, daß diese psycho-biologische Grenze als Problem der Konstruktion von Verweisungssystemen erkannt werden sollte. Soweit ersichtlich,ist die Arbeit von Schnell die einzige in der juristischen Literatur, die expressis verbis auf die "psycho-biologische Grenzen" von Verweisungen aufmerksam macht [61].

2) Verweisungsrelevante Schlußfolgerungen

Geht man davon aus, daß einerseits das Fassungsvermögen ("Kapazität") des Kurzspeichers begrenzt und andererseits auch die Anzahl der verschiedenen Elemente beschränkt ist, so kann damit die absolute Verständnisgrenze bei Verweisungen auf zwei Wegen erreicht werden:

Zum einen kann Länge und Umfang von Normen als Folge von Verweisungen zur "gedanklichen Unfaßbarkeit" führen ("quantitative Komplexität"), zum anderen kann das Zusammenspiel der Verweisungen, d. h. ihre Struktur derart verschachtelt und vernetzt sein, daß dadurch die medizinisch-psychologischen Grenzen erreicht werden ("strukturelle Komplexität").

60) Weltner, Informationstheorie, S. 128 mwN. Ebenso Haft, DSWR 1984, 153; ers. Einführung in das juristische Lernen, S. 11 und S. 14; Dorsch, Psychologisches Wörterbuch, S. 208; Wender/Colonius/Schulze, Modelle des menschlichen Gedächtnisses, S. 26.

61) A. Schnell, 2. Kap. § 3 V. Vgl. auch Haft, Einführung in das juristische Lernen, der auf S. 14 generell auf die Gefahr einer "Informationsüberflutung" aufmerksam macht.

Der erste Fall liegt dann vor, wenn die Verweisungen eine derartige Wortfülle zur Folge haben, daß allein die schlichte Anzahl der Worte das Verständnis unmöglich macht. Um zu zeigen, zu welchem Ergebnis die sprachliche Auflösung der Verweisungen beim BDSG führt, habe ich versucht, die Strafbestimmungen des § 41 BDSG in einem Satz zusammenzufassen ("Definitionsauflösung"). Das Ergebnis wird weiter unten in Abschnitt B vorgestellt werden.

Der zweite Fall ("strukturelle Unbestimmtheit") ergibt sich besonders dann, wenn die Verweisungen nicht linear erfolgen, sondern verschachtelt sind u. komplexe Verzweigungen in sich bergen, was besonders bei Teilverweisungen, bedingten Verweisungen und Mehrfachweisungen der Fall ist [62]. Sie sind, wie Kindermann formuliert, "außerordentlich verwirrend und daher gefährlich", da Umfang und Inhalt der beabsichtigten Regelung häufig nicht exakt genug zu erkennen sind [63]. Das kann dann nicht nur zu einem "Wirrwar" [64] und zu vom Gesetzgeber ungewollten Ringschlüssen und logischen Fehlern, sondern auch schlicht zur Unverständlichkeit der Norm aufgrund dieser Komplexität führen. Um zu überprüfen, ob das speziell beim BDSG der Fall ist, wird in Abschnitt B die von § 41 BDSG ausgehende Struktur der Verweisungen in graphischer Form ("Verweisungsbaum") dargestellt und dann analysiert werden.

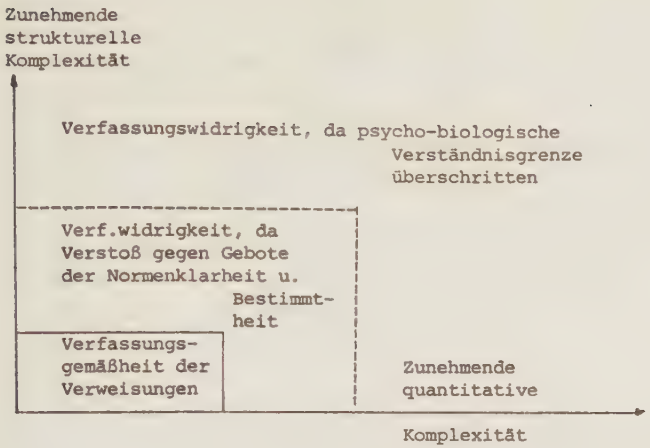
Graphisch läßt sich das Problem der Verfassungswidrigkeit von Verweisungen infolge struktureller und quantitativer Komplexität wie folgt verdeutlicht:

62) Hill S. 115; Kindermann S. 71; Noll S. 231. Beispiele für verwirrende Verweisungen bei Baumann/Dähn, Studien zum Wirtschaftsrecht, S. 58 f.; Noll S. 234 und A. Schnell, Diss. Tü. 1984.

63) Kindermann S. 72.

64) Noll S. 233.

Abb. 3.2 "Komplexitätsfolgen":



B) Die Verweisungen des BDSG

Bevor im empirischen Teil die Frage fehlerhafter Rechtsanwendung erörtert wird, soll in diesem Abschnitt die strukturelle und quantitative Komplexität der Datenschutzgesetze plastisch veranschaulicht sowie erläutert und analysiert werden.

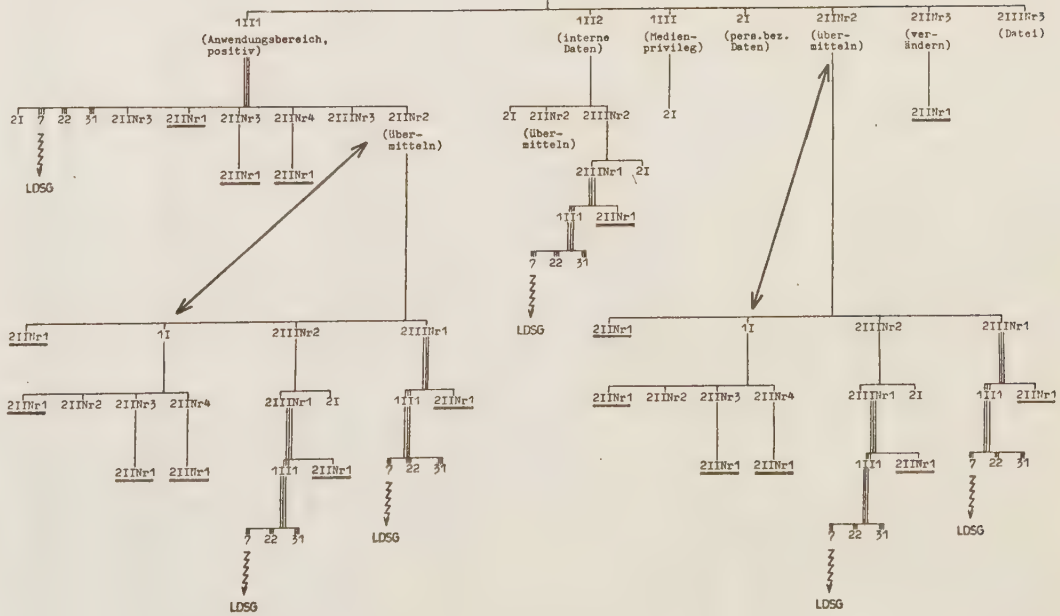
I) Die Darstellung der strukturellen Komplexität anhand eines "Verweisungsbaumes"

Stellt man die von § 41 BDSG ausgehenden Verweisungen graphisch dar, so ergibt sich folgender "Verweisungsbaum":

§ 41 I BDSG

Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,
1. übermittelt oder verändert oder
2. abruft oder sich aus in Behältnissen verschlossenen Dateien verschafft,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.



Erläuterungen:

Zahlen = Paragraphen, Absätze, Sätze (Ziffern) des BDSG

——— = implizite (stillschweigende) Verweisungen

═══ = explizite (ausdrückliche) Verweisungen

≈≈> = dynamische Außenverweisung auf LDSG (d.h. auf das jeweilige Landesdatenschutzgesetz)

<—> = Zirkularität ("zirkuläre Verweisung")

2IINr1 = § 2 II Nr.1 ("speichern") als Verweisungsende

II) Das Ergebnis der Strukturdarstellung

Der vorliegende "Verweisungsbaum" zeigt anschaulich die von § 41 BDSG ausgehende komplexe Struktur der Verweisungstechnik. Nimmt man eine nähere Untersuchung vor, so stößt man auf drei Besonderheiten:

- Erstens die mit der Definition von "speichern" (§ 2 II Nr. 1 BDSG) endenden Verweisungsketten,
- zweitens der Umfang des Anwendungsbereiches des Gesetzes und
- drittens die Struktur der Definition von Übermittlung (übermitteln) in § 2 II Nr. 2 BDSG.

1) Die erste der Besonderheiten ist, daß von den 48 Endpunkten der Verweisungen, siebzehn § 2 II Nr. 1, die Definition von "speichern", zum Gegenstand haben. Selbst wenn man den zweiten Verweis auf die Übermittlungsdefinition und die daraus folgenden Weiterverweisungen auf § 2 II Nr. 1 BDSG nicht dazu rechnen würde, bliebe es bei immer noch zehn Verweisen auf das Wort "speichern". Nach dem Wortlaut des § 41 BDSG stellt das "Speichern" keine Tatmodalität dar, woraus dessen Straflosigkeit gefolgert wird [65]. Mag dies auch zudem der Intention des Gesetzgebers entsprechen [66], so verblüfft dennoch die hohe Zahl der impliziten Verweise auf die Legaldefinition von "Speichern (Speicherung)" in § 2 II Nr. BDSG.

2) Das zweite Charakteristikum betrifft die Dimension des Anwendungsbereichs des Gesetzes. Bei den von § 1 II 1 BDSG (der positiven Umschreibung des Anwendungsbereiches) ausgehenden Verweisungen mag zwar (optisch) zunächst der Eindruck entstehen, daß es sich um eine "einfache" Verweisung handelt,

65) Kamlah in: Burhenne/Perband § 41 RN 11; Dammann in: Simitis/D/M/R §41 RN 9; Louis RN 351.

66) So der auf Gesetzgebungsebene für das BDSG zuständige Referent Auernhammer in seinem Kommentar, § 41 RN 2.

betrachtet man jedoch den Umfang der §§ 7, 22, 31 BDSG, so wird die Komplexität allein aufgrund der Anzahl der Worte einsichtig [67]. Doch nicht allein diese quantitative Komplexität, sondern besonders die strukturelle offenbart sich, denn nach § 7 II BDSG gilt das BDSG (im öffentlichen Bereich) nur "soweit der Datenschutz nicht durch Landesgesetz geregelt ist". Die Subsidiaritätsregelung [68] des § 7 II BDSG ist nämlich das Einfallstor für die Verweisungsketten der jeweiligen Landesdatenschutzgesetze. Weiter unten bei der Auswertung wird gezeigt werden, daß Polizei und Staatsanwaltschaft gerade bei der Frage des Anwendungsbereiches besonders oft Fehler unterliefen.

3) Die dritte Besonderheit schließlich zeigt sich bei einer streng formalen Untersuchung. Dazu ist die Auflösung der Definition von § 2 II Nr. 2 BDSG ("übermitteln") - einem Zentralbegriff des Gesetzes - [69] notwendig. Ersetzt man die Begriffe jeweils durch ihre Erklärungen, so offenbart sich das unter formalen Gesichtspunkten interessanteste Ergebnis:

§ 2 II Nr. 2 BDSG lautet:

"Im Sinne des Gesetzes ist übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an Dritte ..."

Löst man nun die in § 1 I BDSG gebrauchte Legaldefinition von

"Datenverarbeitung"
= Speicherung, Übermittlung, Veränderung und Löschung

auf und fügt sie in die obige Definition ein, so ergibt das die folgende Definition:

67) Vgl. Haft, DSWR 1979, 139, der darlegt, daß § 7 BDSG aus 183, § 22 aus 153 und § 31 aus 264 Wörtern besteht.

68) Von einer "Vorrangklausel" spricht z. B. Dammann in Simitis/D/M § 7 RN 43.

69) Tubies DuD 1979, 157; Kröger, BDSG, C. II (S. 15).

Übermittlung = das Bekanntgeben gespeicherter oder durch Speicherung, Übermittlung, Veränderung und Löschung unmittelbar gewonnener Daten an Dritte ...

Es taucht also in der Definition der Begriff auf, der definiert werden soll. Damit wurde gegen das Zirkularitätsverbot verstoßen, das besagt, daß in einer Definition nicht der Begriff vorkommen darf, der definiert werden soll [70]. Es entsteht nach Auflösung zwar keine tautologische Relation [71] im Sinne von

Übermittlung = Übermittlung,

aber es wird ein Verstoß gegen das Zirkularitätsverbot [72] sichtbar, denn die entsprechende Formulierung lautet hier:

Übermittlung = das Bekanntgeben ... durch Übermittlung ... gewonnener Daten.

Es liegt also ein - wie Klug formuliert - Verstoß gegen die "logische Korrektheit einer Definition" vor [73]. Fraglich ist, ob dieser formale Verstoß nicht das rechtsstaatliche Gebot der Normenklarheit und zugleich das strafrechtliche Bestimmt-

70) Rödig in: Schriften zur juristischen Logik S. 312; Klug Jurist. Logik S. 105; ders. in: Gedächtnisschrift für Rödig S. 205; von Savigny S. 116. Ebenso Kindermann S. 65: Er bezeichnet das Zirkelverbot neben dem Verbot der Mehrfachdefinition und dem Verbot der nachträglichen Interpretation als wichtigste Definitionsregel, die auch in nichtformalisierten Systemen beachtet werden müßten.

71) Tautologisch und damit lediglich überflüssig könnte man dagegen die Formulierung in § 31 I Nr. 1 BDSG nennen, in der es heißt:
"... Daten zum Zwecke der Übermittlung ... übermitteln ...".

72) Als Beispiel mit dem gleichen Fehler führt Klug, Jurist. Logik S. 106 und ders. in Gedächtnisschrift Rödig S. 205, an: "Eisenbahn ist eine Eisenbahn zwecks Bewegung von Gegenständen".

73) Klug, Gedächtnisschrift für Rödig S. 204; er führt auf S. 205 als weitere Beispiele für den Verstoß gegen die logische Korrektheit einer Definition neben dem Zirkelverbot das Verbot der Mehrfachdefinition und das Verbot der nachträglichen Interpretation an.

heitsgebot verletzt [74]. Man wird jedenfalls nicht soweit gehen können, anzunehmen, daß dieser formale Fehler in der Definition eines - wenn auch zentralen - Begriffes des BDSG für sich allein genommen zur Verfassungswidrigkeit des gesamten Gesetzes führt [75]. Gleichwohl begegnen einer strafrechtlichen Verfolgung wegen unbefugter Datenübermittlung erhebliche verfassungsrechtliche Zweifel [76].

Für alle Landesdatenschutzgesetze außer denen in Hamburg, Hessen und Nordrhein-Westfalen, da dort nicht "Datenverarbeitung" definiert wird, gilt das eben Ausgeführte in gleicher Weise. In Hamburg, mit dem jüngsten Landesdatenschutzgesetz [77], wurde jedoch der strukturell gleiche Fehler mit der Definition von "Verarbeiten" begangen, da in § 4 II HmbDSG die "Verarbeitung" als "Sperren" und in § 4 III HmbDSG das "Sperren" als "Verhinderung weiterer Verarbeitung" definiert wurde.

Warum dieser logische Fehler in der Übermittlungsdefinition entstanden ist, läßt sich wohl kaum erklären, um so erstaunlicher ist aber, daß er seit über 10 Jahren unbemerkt geblieben ist, denn schon der Gesetzesentwurf der Bundesregierung vom 21.9.1973 [78] enthielt diesen Verstoß gegen das Zirkularitätsverbot:

74) Man kann auch nicht unterstellen, daß der Begriff "Datenverarbeitung" in § 1 I BDSG anders zu verstehen ist, als in § 2 II Nr. 2 BDSG. Es sind keine Anhaltspunkte vorhanden, warum der im ersten Paragraphen definierte Begriff im zweiten plötzlich nicht mehr gelten soll.

75) Demgegenüber aber Kindermann S. 59: "Ist die Definition eines Gesetzes falsch, so gerät das Gesetz ins Wanken.".

76) Dasselbe wird man wohl für die Tatmodalität "abrufen" in § 41 I Nr. 2 BDSG annehmen müssen, da das Merkmal nicht nur in einem engen Zusammenhang mit der "Übermittlung" steht, sondern sogar in dieser Definition vorkommt, denn nach § 2 II Nr. 2 BDSG ist "übermitteln", "das Bekanntgeben gespeicherter Daten ... in der Weise, daß die Daten ... zur Einsichtnahme, namentlich zum Abruf bereitgehalten werden". Vgl. zum Datenabruf die ausführliche Darstellung von Ringwald, JZ 1983, 291 ff.; ders. INPOL und StA, § 3.

77) Hamburgisches Datenschutzgesetz (HmbDSG) vom 31.3.1981 HmbGVBl S. 71.

78) BT-Drs. 7/1027.

Dort wurde in § 3 II in der Nr. 1 bestimmt [79]:

"Im Sinne des Gesetzes ist Datenverarbeitung (Verarbeitung von Daten) das Speichern, Verändern, Weitergeben oder Löschen von Daten"

und in Nr. 4:

"Im Sinne des Gesetzes ist Weitergeben (Weitergabe) das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an ...".

Man sieht sofort, daß strukturell der gleiche Fehler vorlag.

Der Bundesrat, dem dieser Gesetzesentwurf der Bundesregierung von 1973 zur Stellungnahme vorlag, sah den Fehler ebenfalls nicht, obwohl er sich mit den Legaldefinitionen, insbesondere der von "Datenverarbeitung", auseinandergesetzt und folgende Anregung gegeben hatte [80]:

"In § 3 Abs. 2 wird der Terminus 'Datenverarbeitung' legal als das 'Speichern, Verändern, Weitergeben oder Löschen von Daten' definiert. Gleichwohl verwendet der Gesetzentwurf in einer Reihe von Bestimmungen (z. B. § 5 Abs. 3 Satz 1, § 13 Abs. 1, § 16 Abs. 1 und 2 und § 23 Nr. 3) die Ausdrücke 'Speichern' und 'verarbeiten' nebeneinander. Diese Tautologie ist nicht nur überflüssig, sondern führt in einigen Bestimmungen auch zu Unklarheiten und Divergenzen. Die Bundesregierung wird daher gebeten, die entsprechenden Bestimmungen des Gesetzentwurfes im Hinblick auf die Legaldefinition in § 3 Abs. 2 zu überarbeiten."

Als nach fast 3 Jahren Beratungen auf Antrag des Innenausschusses am 2.6.1976 die Definition von "Datenverarbeitung" in einen anderen Paragraphen ausgelagert wurde und - wie es in der Begründung wörtlich heißt - der Begriff "weitergeben" durch den umfassenderen Begriff "übermitteln" ersetzt wurde [82]

79) BT-Drs. 7/1027 S. 5.

80) BT-Drs. 7/1027 Anlage 2 S. 33 (= "Zu § 3").

81) BT-Drs. 7/1027 S. 6 (= "Zu § 2").

82) Der Begriff "weitergeben" wurde jedoch durch den Vermittlungsausschuß nicht vollständig ersetzt, wie § 2 II Nr. 2 BDSG zeigt: "Übermitteln (ist) das Bekanntgeben ... gewonnener Daten ... in der Weise, daß die Daten ... weitergegeben ... werden."

(was wiederum zur "redaktionellen Änderung der Strafbestimmung" führte, da auch dort der Begriff "weitergeben" durch "übermitteln" ersetzt wurde) [83], war dieser Verstoß gegen das Zirkularitätsverbot immer noch nicht bemerkt worden.

Im (inzwischen zurückgezogenen) Referentenentwurf vom 23.6.1983 war nun vorgesehen, den Übermittlungsbegriff zu modifizieren [84]; der Fehler war aber auch darin unverändert enthalten.

III) Die Darstellung der quantitativen Komplexität anhand der sprachlichen Auflösung der Definitionen

Nachdem nun ausgehend vom oben dargestellten "Verweisungsbaum" [85] die Verweisungsketten in bezug auf ihre strukturelle Komplexität analysiert wurden, erfolgt nunmehr eine sprachliche Auflösung zur Feststellung der quantitativen Komplexität. Dabei wird - ungeachtet des bei § 2 II Nr. 2 BDSG vorhandenen Verstoßes gegen das Zirkularitätsverbot [86] - versucht, die verschiedenen Verweisungen auf Definitionen und Paragraphen möglichst vollständig aufzulösen, d. h. die Normen und Begriffe in ihrem Wortlaut wiederzugeben, so daß schließlich die Strafbestimmung in einem Satz der alle nötigen Informationen enthält, zusammengefaßt ist.

Bei dieser Methode zur Feststellung der quantitativen Komplexität mußten Unformulierungen vorgenommen werden. So war z. B. die Transformation der Definition von "speichern", die in Infinitiv- bzw. Substantiv-Form vorliegt, für die Fälle nötig, in denen von "gespeicherten" Daten die Rede ist. Entscheidend war jedoch nicht die exakte, sprachlich einwandfreie Umformulierung, sondern zentrales Anliegen war die Darstellung der Ergebnisse zu denen die Auflösung führt.

83) BT-Drs. 7/1027 S. 11 (= "Zu § 32").

84) Abgedruckt in DANA 5/1983 S. 5 - 10. Das Volkszählungsurteil des BVerfG (E 65, 1 ff.) war wohl der Grund dafür, daß er zurückgezogen wurde: vgl. computer magazin, Heft 6, 1984 S. 6.

85) siehe oben, § 3 B I der Arbeit.

86) Dazu oben, § 3 B II 3) der Arbeit.

Die Einbeziehung mehrfach vorkommender gleicher Definitionen wurde vermieden. Wird eine Definition mehrfach gebraucht (es wurde schon oben ausgeführt, daß z. B. auf "speichern" siebzehnmal verwiesen wird) [87] so wurde sie nur beim erstenmal aufgelöst.

Damit die inhaltliche Verständlichkeit gewahrt bleibt, wurde § 41 Abs. 1 geringfügig umgestellt, damit die Ersetzung der definierten Begriffe ("Auflösung") nicht zur sprachlichen Umcodierung führt.

§ 41 BDSG lautet:

"Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind, ...".

Nach der Umstellung lautet § 41 BDSG nunmehr:

"Wer unbefugt personenbezogene Daten, die dieses Gesetz schützt, die nicht offenkundig sind, ...",

Der Grund für diese Maßnahme lag darin, daß damit die Formulierung, die den Anwendungsbereich festlegt (§ 1 II BDSG: "Dieses Gesetz schützt ...") ohne sprachliche Umwandlung verwandt werden konnte.

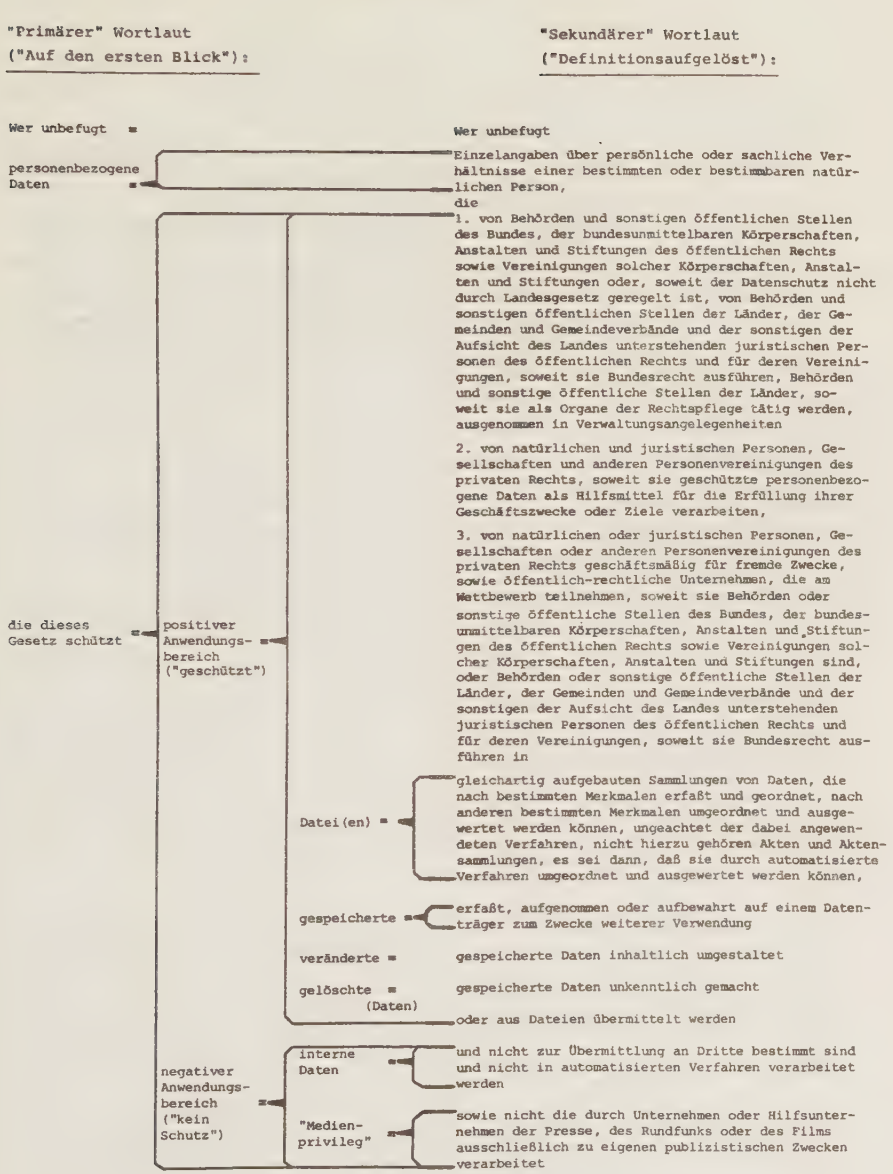
Ausgangspunkt ist damit folgender Satz:

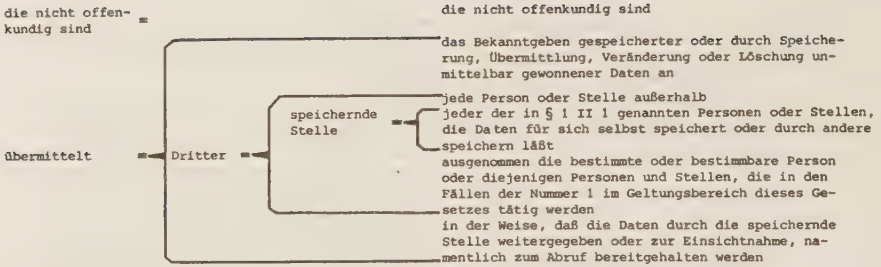
Wer unbefugt
personenbezogene Daten,
die dieses Gesetz schützt,
die nicht offenkundig sind,
übermittelt oder verändert oder
abruft oder sich aus in Behältnissen
verschlossenen Dateien verschafft,
wird mit Freiheitsstrafe bis zu einem
Jahr oder mit Geldstrafe bestraft.

87) Vgl. oben, § 3 B I, die Abb. 3.3 "Verweisungsbaum" mit den Erläuterungen und im Text § 3 B II.

Führt man nun die Verweisungen durch und löst die Definitionen auf, wobei allerdings die sprachliche Umwandlung der gegen das Zirkularitätsverbot verstoßenden Defintion von Übermittlung (übermitteln) in die entsprechende Form von "übermittelt" unterblieb, so ergibt sich folgende Strafbestimmung:

§ 41 BDSG


"Primärer" Wortlaut
("Auf den ersten Blick"):
"Sekundärer" Wortlaut
("Definitionsaufgelöst"):
Wer unbefugt =
Wer unbefugt
personenbezogene Daten =
Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person,
die
1. von Behörden und sonstigen öffentlichen Stellen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie Vereinigungen solcher Körperschaften, Anstalten und Stiftungen oder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist, von Behörden und sonstigen öffentlichen Stellen der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen, soweit sie Bundesrecht ausführen, Behörden und sonstige öffentliche Stellen der Länder, soweit sie als Organe der Rechtspflege tätig werden, ausgenommen in Verwaltungsangelegenheiten
2. von natürlichen und juristischen Personen, Gesellschaften und anderen Personenvereinigungen des privaten Rechts, soweit sie geschützte personenbezogene Daten als Hilfsmittel für die Erfüllung ihrer Geschäftszwecke oder Ziele verarbeiten,
3. von natürlichen oder juristischen Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts geschäftsmäßig für fremde Zwecke, sowie öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, soweit sie Behörden oder sonstige öffentliche Stellen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie Vereinigungen solcher Körperschaften, Anstalten und Stiftungen sind, oder Behörden oder sonstige öffentliche Stellen der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen, soweit sie Bundesrecht ausführen in
die dieses Gesetz schützt =
positiver Anwendungsbereich ("geschützt") =
Datei(en) =
gleichartig aufgebauten Sammlungen von Daten, die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden können, ungeachtet der dabei angewendeten Verfahren, nicht hierzu gehören Akten und Aktensammlungen, es sei dann, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können,
gespeicherte =
erfaßt, aufgenommen oder aufbewahrt auf einem Datenträger zum Zwecke weiterer Verwendung
veränderte =
gespeicherte Daten inhaltlich umgestaltet
gelöschte = (Daten)
gespeicherte Daten unkenntlich gemacht
oder aus Dateien übermittelt werden
negativer Anwendungsbereich ("kein Schutz") =
interne Daten =
und nicht zur Übermittlung an Dritte bestimmt sind und nicht in automatisierten Verfahren verarbeitet werden
"Medienprivileg" =
sowie nicht die durch Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Films ausschließlich zu eigenen publizistischen Zwecken verarbeitet



oder verändert	oder verändert
oder abruft	oder abruft
oder sich aus in Behältnissen verschlossenen Dateien verschafft	oder sich aus in Behältnissen verschlossenen Dateien verschafft
wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.	wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
Handelt der Täter gegen Entgelt oder in der Ansicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.	Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.
Die Tat wird nur auf Antrag verfolgt.	Die Tat wird nur auf Antrag verfolgt.

IV) Das Ergebnis der sprachlichen Auflösung

Man hat nun eine Strafbestimmung, die nach Auflösung der Verweisungen und Definitionen von 36 auf 421 Worte gewachsen ist [88]. Es ist fraglich, ob eine derartig verschachtelte und komplexe Norm (abgesehen vom Verstoß gegen das Zirkularitätsverbot) für sich betrachtet noch dem strafrechtlichen Bestimmtheitsgebot und/oder dem rechtsstaatlichen Gebot der Normenklarheit entspricht. Weiter ist jedoch zu bedenken, daß die so gewonnene Norm nur den Kern der Strafbestimmung darstellt, da das BDSG gemäß § 7 II BDSG nur insoweit gilt, als "der Datenschutz nicht durch Landesgesetz geregelt ist" [89]. Folglich muß man (sofern der öffentliche Bereich betroffen ist) zuerst das jeweilige Landesdatenschutzgesetz in der eben dargestellten Weise auflösen, es gedanklich aufnehmen, dann die obige BDSG-Auflösung bewältigen um danach durch Vergleich festzustellen, ob eines der Gesetze, und wenn ja, welches, einschlägig ist. Doch auch mit dieser Operation ist die Frage des Anwendungsbereiches nicht endgültig geklärt, da noch festzustellen ist (und dies gilt auch für den nichtöffentlichen Bereich), ob gemäß § 45 BDSG vorrangige Rechtsvorschriften existieren. Es ist höchst zweifelhaft, ob der Regelungskomplex der Datenschutzgesetze mit diesem Verweisungswirrwar [90] im Hinblick auf das rechtsstaaatliche Gebot der Normenklarheit und der für Strafnormen erforderlichen "besonders strengen Anforderungen die Bestimmtheit" [91] noch verfassungsgemäß ist.

88) Schlapp, JuS 1984, 508 FN 36, bezeichnet den nur unwesentlich kürzeren § 1 KSchG als "Monsternorm".

89) Nach Dammann, NJW 1978, 1907 gerät die Rechtseinheit durch solche Vorrangklauseln in Gefahr. Vgl. auch den gleich strukturierten § 1 III BVwVfG und die dazu bestehende Literatur.

90) Noll, Gesetzgebungslehre, S. 233.

91) So die Formulierung des BayVerfGH in BayVGH Bd. 67 (= Bd. 4 n. F.) S. 90, 106. Ähnlich Kindermann S. 34 und Tiedemann NJW 1980, 1559; ers. Tatbestandsfunktionen, S. 197 f., 242 mwN.

Daß gerade die von der Subsidiaritätsfrage des § 7 II BDSG (und des § 45 BDSG) ausgehenden Abgrenzungs- und Verweisungsschwierigkeiten für die Frage einer Bestrafung entscheidend sein könne, zeigt nicht nur das Urteil des LG Bad Kreuznach [92], sondern auch die Tatsache, daß dieses Problem in einigen der hier ausgewerteten Verfahren expressis verbis angeschnitten wurde. Zur Verdeutlichung das folgende Verfahren:

Fall 1 ("Der Universitätsoperator"):

Der seit 10 Jahren im Rechenzentrum einer Universität als Steuerpultbediener angestellte Operator O kopierte, teilweise außerhalb, teilweise innerhalb der Dienstzeit, drei Magnetbänder, welche die kompletten Personaldaten der an der Hochschule Beschäftigten enthielten und stellte dann von den kopierten Bändern Mikrofiches im COM-Verfahren 93 her, deren genaue Anzahl sich nicht mehr feststellen ließ, da die Maschinenprotokolle teilweise von ihm vernichtet worden waren. O war auf das Datengeheimnis nach dem Landesdatenschutzgesetz verpflichtet worden, wie aus der in der Akte beigefügten Kopie ersichtlich war.

Durch einen Zufall stieß man in seinem Schreibtisch auf die drei Magnetbänder und weiteres belastendes Material. Nach hochschulinternen Ermittlungen und "Vernehmungen" des O wurde dieser entlassen und die Angelegenheit der Staatsanwaltschaft übergeben. Der Rektor stellte dann nach Rücksprache mit der Staatsanwaltschaft Strafantrag. Eine richterlich angeordnete Hausdurchsuchung nach Beweismaterial blieb erfolglos. Bei der Vernehmung gab er als Grund für sein Verhalten an, er habe lediglich experimentieren und die Verfilmung testen wollen. Die Staatsanwaltschaft erließ daraufhin einen Strafbefehl, in dem O beschuldigt wurde, er habe "fortgesetzt aus der Datei einer öffentlichen Stelle unbefugt personenbezogene Daten, die nicht offenkundig sind, abgerufen", indem er drei Magnetbänder mit den kompletten Personaldaten kopierte und von den kopierten Bändern Mikrofiches hergestellt habe.

Dies sei "ein Vergehen nach §§ 1, 41 I Ziff. 2 Datenschutzgesetz", weshalb eine Geldstrafe in Höhe von 50 Tagessätzen festgesetzt werde.

Der Beschuldigte legte keinen Einspruch ein, sondern akzeptiere den Strafbefehl sofort.

Bei der Bestimmung der maßgebenden Strafnorm ist im vorliegenden Fall von § 7 Abs. 2 BDSG auszugehen. Danach "gelten für Behörden und sonstige öffentliche Stellen die Vorschriften des 2. Abschnittes mit Ausnahme der §§ 15 - 21 für Behörden und

92) NJW 1978, 1931 f.

93) Computer-output-mikrofiche. Dazu Schott DSWR 1983, 21 ff.

sonstige öffentliche Stellen der Länder ..., es sei denn, sie nehmen am Wettbewerb teil, soweit der Datenschutz nicht durch Landesgesetz geregelt ist". Nach § 7 Abs. 3 BDSG gelten abweichend von Abs. 2 anstelle der §§ 9 - 14 die §§ 23 - 27, soweit dienst- oder arbeitsrechtliche Rechtsverhältnisse betroffen sind. Der Gesetzgeber begründet die Regelung des § 7 III BDSG damit, daß "alle Arbeitsverhältnisse datenschutzrechtlich einheitlich" behandelt werden sollen [94]. Damit wird aber nur festgelegt, welche Regelungen für die Datenverarbeitung gelten, nicht aber, wie ein Verstoß dagegen zu bestrafen ist:

In Betracht kommt zum einen die Landesstrafbestimmung, weil es sich bei der Universität um eine Datei einer öffentlichen Stelle des Landes handelt, bei der zudem der Täter angestellt ist. Andererseits spricht für die Bundesstrafbestimmung, daß es sich um Personaldaten handelt.Letzteres hätte zur Konsequenz, daß bei gleichzeitigem Zugriff auf andere als Personaldaten das Landesdatenschutzgesetz (neben dem BDSG) gelten könnte, womit dann die Datenart relevant würde und nicht die Datei. Erfüllt hier O auch noch die Täterqualifikationen des § 203 StGB, so wird auch diese Vorschrift über die "auf dem Hintergrund des bestehenden methodischen Instrumentariums der Rechtswissenschaft Schwierigkeiten auslösende Subsidiaritätsklausel" [95] des § 45 BDSG zu prüfen sein [96].

Die Entscheidung soll hier bewußt offen gelassen werden, denn der Fall soll nur das zu einem Verweisungschaos führende Prinzip der Subsidiaritäts- bzw. Unterausnahmeregelungen demonstrieren, das durch mangelnde Klarheit und Unbestimmtheit verfassungsrechtlich äußerst bedenklich ist.

94) BT-Drs. 7/1027 S. 24 (= "Zu § 5").

95) Hümmerich DVR 1977, 130. Ähnlich Sendler DuD 1977, 63. Zur Kritik an dem in diesem Zusammenhang verwendeten Begriff "Subsidiarität" Tonnies DuD 1981, 25.

96) In Bayern ist zudem noch die Strafbestimmung des Art. 16 des Gesetzes über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern (vgl. Art. 35 BayDSG) zu beachten.

C) Exkurs: Die Strafbestimmung des Sozialgesetzbuches und die Darstellung ihrer Verweisungskomplexität

Noch verwirrender und komplexer sowohl in struktureller als auch quantitativer Hinsicht ist der strafrechtliche Schutz der Sozialdaten geregelt [97]. Bedenkt man, daß neunzig Prozent der Bürger direkt oder indirekt vom System der sozialen Sicherheit erfaßt werden [98], so ist der Kritik am neuen, 10. Buch des Sozialgesetzbuches (SGB X) vom 18.8.1980 [99] besondere Beachtung zu schenken [100]. So wird diesem bereichsspezifischen Datenschutzgesetz [101] mangelnde Transparenz [102] und ein schwer bestimmbarer Anwendungsbereich [103] vorgeworfen und Schedl hält sogar "zumindest das 2. Kapitel des Gesetzes (§§ 67 - 85) für überflüssig" [104].

In § 79 I SGB X findet sich nun auch eine Verweisung auf die Strafbestimmung des § 41 BDSG:

97) Gesetz ist so "perfekt", daß nicht einmal Abteilungsleiter von Arbeitsämtern wissen, was sie dürfen, und was nicht. So hielt sich ein polizeilich gesuchter Räuber zwecks Gewährung sozialer Hilfe im Arbeitsamt auf. Eine Angestellte verständigte telefonisch die Polizei. Als sie dies ihrem Abteilungsleiter mitteilte, schickte dieser den Antragsteller vor Eintreffen der Polizei weg. Der Abteilungsleiter wurde wegen Strafvereitelung (§ 258 StGB) angeklagt und schließlich vom Berufungsgericht aus subjektiven Gründen freigesprochen. Vgl. den Jahresbericht 1982 des Berliner Datenschutzbeauftragten, Drs. 9/885 vom 29.12.1982 des Abgeordnetenhauses von Berlin, S. 14; ferner dazu: Kerkau DuD 1983, 109 f. und Wimmer, Datenschutz in der öff. Verwaltung, S. 64.

98) Heussner, FS Wannagat, 1981 S. 191.

99) BGBl. I S. 1469.

100) Dies bestätigt auch die Auswertung, vgl. § 5 A IV der Arbeit.

101) Wiese ÖVD 1981, 11 ff.; vgl. dazu auch Küppers DuD 1980, 1985 ff. und Grassl/Weigert DuD 1981, 76 ff.; dies. DSWR 1981, 113 ff., 140 ff., 186 ff.; Rische DRV 1980, 379 ff.

102) Karrer, Kommunalpraxis 1981, 180.

103) Sachau, der bayr. Bürgermeister 1981, 18; Mallmann/Walz NJW 1981, 1024 "nicht zu verkennende Verkomplizierung".

104) Schedl DSWR 1981, 284.

§ 79 SGB X:

(1) Die in § 35 des Ersten Buches genannten Stellen unterliegen, soweit sie personenbezogene Daten oder Betriebs- oder Geschäftsgeheimnisse in Dateien verarbeiten, nach Maßgabe der §§ 80 - 85 den Vorschriften des Ersten und Zweiten Abschnitts sowie den §§ 41, 42 Abs. 1 Nr. und § 45 des Bundesdatenschutzgesetzes; die §§ 28 und 29 des Bundesdatenschutzgesetzes sind entsprechend anzuwenden.

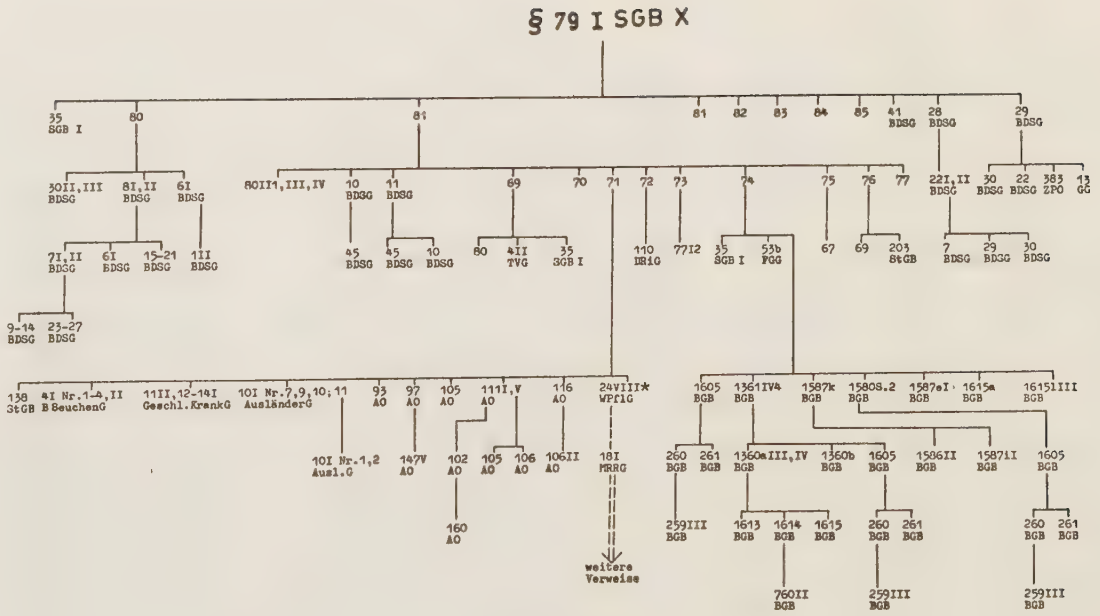
(2) Für Krankenhäuser und Einrichtungen zur Eingliederung Behinderter gelten abweichend vom § 7 Abs. 1 Satz 2 und Abs. 2 auch die §§ 8, 9 und 12 bis 14 des Bundesdatenschutzgesetzes.

(3) Die Vorschriften des Zweiten Abschnitts des Bundesdatenschutzgesetzes gelten abweichend von § 7 Abs. 2 Satz 1 auch, soweit der Datenschutz durch Landesgesetz geregelt ist. An Stelle des Bundesbeauftragten für den Datenschutz treten insoweit die nach Landesrecht zuständigen Stellen.

Den Versuch, die von Absatz 2 ausgehenden Verweisungen nachzuvollziehen, unternimmt Wochner und kommt zu dem Ergebnis, daß "das Durcheinander perfekt" sei [105].

Der auf § 41 BDSG verweisende Absatz 1 enthält eine ganze Reihe expliziter Außen- und Binnenverweisungen. Ausgehend von ihm soll hier nur kurz graphisch dargestellt werden, wie "leicht" sich ermitteln läßt, welche Sozialdaten (sowie Betriebs- und Geschäftsgeheimnisse) wann und von welchem Gesetz (auch § 203 StGB ist zu beachten) geschützt sind (wobei nur die expliziten Verweisungen dargestellt werden):

105) Wochner DVBl 1982, 235. Auch nach Grassl/Weigert DSWR 1981, 187 ist "die Reichweite dieser Bestimmung problematisch".



Erläuterungen:

Zahlen ohne weitere Angaben = §§ des SGB X; Zahlen mit Angaben = §§ der jeweils genannten Gesetze.

---

* Der Verweis auf Abs. 8 des § 24 WPflG ist verfehlt; gemeint ist wohl Abs. 9.

§ 4

Grundlagen und Methodik der empirischen Auswertung einschliesslich deren Verfahrenscharakteristika

In diesem Kapitel der Arbeit wird zunächst dargestellt, wie die 159 ausgewerteten Verfahren erlangt wurden (Abschnitt A - Grundlagen -) und die methodische Vorgehensweise bei der Analyse erläutert (Abschnitt B - Methodik -). Danach erfolgt eine kurze Darstellung einiger Verfahrenseigenschaften, um die Art und Beschaffenheit des verarbeiteten Materials besser einschätzen zu können (Abschnitt C - Verfahrenscharakteristika-).

A) Grundlagen der Auswertung

Ausgangspunkt der Untersuchung war zunächst die Statistik des Bundeskriminalamtes (BKA), nach der innerhalb der ersten fünf Jahre seit dem Inkrafttreten des BDSG [1], nämlich von 1978 - 1982, insgesamt 219 Straftaten unter der Rubrik "Straftaten gegen das Bundes- (oder Landes-) Datenschutzgesetz" registriert waren [2].

Die Aufgliederung dieser BKA-Statistik nach Bundesland und Jahr ergibt sich aus der Tabelle 4.1:

1) Das Gesetz trat am 1.1.1978 in Kraft (§ 47 BDSG).

2) Polizeiliche Kriminalstatistik 1978,1979, 1980, 1981, 1982. Hrsg.: BKA - Kriminalistisches Institut, Wiesbaden. Zur Problematik von Kriminalstatistiken grundlegend Göppinger, Kriminologie, S. 136 - 156; vgl. auch Dästner S. 15 - 19 und Heinz wistra 1983, 129.

Tabelle 4.1 "BKA-Statistik":

Bundesland	erfaßte Fälle					
	1978	1979	1980	1981	1982	insges.
Baden-Württ.	2	3	6	3	2	16
Bayern	1	4	3	7	9	24
Berlin	1	2	2	3	0	8
Bremen	1	0	0	2	1	4
Hamburg	1	2	2	1	0	6
Hessen	4	3	6	10	7	30
Niedersachsen	0	7	4	10	6	27
Nordrh. Westf.	4	10	23	25	23	85
Rheinl. Pfalz	0	0	3	4	3	10
Saarland	0	0	0	1	2	3
Schl. Holst.	0	3	2	1	0	6
Bundesgebiet	14	34	51	67	53	219

I) Erlangung der Akten und Einsichtnahme

Das BKA speichert selbst keine Aktenzeichen von Verfahren, da es nur die Anzahl der jeweils von den Landeskriminalämtern gemeldeten Verstöße sammelt und akkumuliert. So wurden alle zentralen Dienststellen der Kriminalpolizei (Landeskriminalämter) in den Ländern angeschrieben, um von dort eine Aufstellung der Aktenzeichen zu erhalten. Gleichzeitig wurden die jeweils zuständigen Behörden der Länder [3] um Genehmigung zur Akteneinsicht ersucht.

Daraufhin übermittelten sieben Landeskriminalämter [4] die einschlägigen Aktenzeichen. Zwar hätten es nach den BKA-Statistiken in diesen fünf Jahren 53 Aktenzeichen sein müssen, doch

3) Vgl. im einzelnen Nr. 182 ff. RiStBV (Richtlinien für das Strafverfahren und das Bußgeldverfahren). Abgedruckt als Anhang in den meisten StPO-Kommentaren.

4) Baden-Württemberg, Berlin, Bremen, Hamburg, Rheinland-Pfalz, Saarland und Schleswig-Holstein.

reduzierte sich nach internen Bereinigungen von "statistischen Fehlerfassungen" der Landeskriminalämter die Zahl auf 38 Aktenzeichen. Nachdem sich bei den Staatsanwaltschaften 5 weitere Fälle als Erfassungsfehler herausgestellt hatten, blieben 33 Verfahren für die Analyse übrig.

Die Landeskriminalämter von Bayern und Hessen konnten keine Aktenzeichen oder sonstige Angaben mitteilen, die zur Identifizierung der von ihnen dem BKA gemeldeten 54 Verfahren hätten führen können. Deshalb mußte in diesen Ländern bei allen Staatsanwaltschaften angefragt werden, mit der Folge, daß schließlich 43 Fälle ausgewertet werden konnten. Hierbei wurde auch der "Verlust" von einigen Verfahren bekannt. Denn bei einer großen Staatsanwaltschaft ging beim Umzug des für Datenschutz-Straftaten zuständigen Dezernenten, dessen intern geführte Liste mit ca. 20 Verfahren verloren. Da die Aktenzeichen dieser Verfahren nicht wieder zu ermitteln waren, entstand dieser "Verlust". Wie er erklärte, seien aber fast alle nach § 170 II StPO eingestellt worden und er erinnere sich noch an einen Fall, bei dem eine Einstellung nach § 153 (a?) StPO erfolgt sei: Ein Polizeibeamter habe - so wörtlich - "seinem Schwiegervater am Terminal gezeigt, was sein neuer Schwiegersohn alles auf dem Kerbholz habe".

Das LKA Niedersachsen übersandte einen Computerausdruck, auf dem Tagebuch-Nummer und Polizeidienststellen von 20 Ermittlungsverfahren abgedruckt waren. Davon stellten sich schließlich 17 Fälle als einschlägig für die Auswertung heraus.

Das Landeskriminalamt Nordrhein-Westfalen übersandte eine Liste mit den Namen von den 30 Polizeibehörden, die Verstöße gegen das Bundes- oder Landesdatenschutzgesetz gemeldet hatten. Nach Anschreiben dieser Polizeibehörden wurden 23 Aktenzeichen direkt mitgeteilt und weitere 16 nach Weiterleitung der Schreiben an die zuständigen Staatsanwaltschaften. Diese 39 Aktenzeichen führten zur Auswertung von 37 Fällen, da sich zwei als Erfassungsfehler herausstellten.

Insgesamt wurden so über die Mithilfe aller Landeskriminalämter 130 Ermittlungsakten erlangt. Da aber die Staatsanwaltschaften nicht nur um Übersendung dieser 130 Akten gebeten wurden, sondern auch um aller der ihnen bis Ende 1982 bekannten Verfahren, konnten weitere 32 Aktenzeichen in Erfahrung gebracht werden. Sie wurden zum überwiegenden Teil von größeren Staatsanwaltschaften mit eigenem Dezernenten für Datenschutz-Strafsachen mitgeteilt.

Ganz vereinzelt wurde in den Tätigkeitsberichten von Landesdatenschutzbeauftragten auf Strafverfahren hingewiesen [5]. Davon konnte der im Bericht des niedersächsischen Landesdatenschutzbeauftragten erwähnte Fall, dessen Sachverhalt dort wie folgt wörtlich abgedruckt ist, nicht erlangt werden [6]:

Fall 2 ("Steuerunterlagen"):

"Der Hausmeister im Gebäude einer Nebenstelle des Ordnungsamtes stand im Verdacht, sich Zugang zu einem verschlossenen Büroschrank verschafft und Einblick in steuerliche Daten seiner Ehefrau genommen zu haben. Die Staatsanwaltschaft hat das Verfahren mangels Vorliegen eines Strafantrages der Betroffenen und mangels öffentlichen Interesses (§ 21 III NDSG) nach § 170 II StPO eingestellt. Die Auffassung der betroffenen Gemeinde, auch sie sei als Verletzte im Sinne von § 77 StGB antragsberechtigt, wurde von der Staatsanwaltschaft nicht geteilt."

5) So in den Tätigkeitsberichten der Landesdatenschutzbeauftragten von Bremen und Niedersachsen. Bezüglich Niedersachsen: IV. Tätigkeitsbericht des Niedersächsischen Datenschutzbeauftragten (Landtags-Drs. 10/720) vom 1.1. - 31.12.1982 RN 12.8 (= S. 55).
Bezüglich Bremen: 3. Jahresbericht, Bremische Bürgerschaft, Drs. 10/483 vom 31.3.1981, S. 47 und 57; 4. Jahresbericht Drs. 10/800 vom 31.3.1982, S. 44; 5. Jahresbericht Drs. 10/1076 vom 31.3.1983, S. 53. Über das zunächst angeschriebene Landeskriminalamt und den Leitenden Oberstaatsanwalt waren mir drei Verfahren zugänglich gemacht worden. Inwieweit diese mit den in den Jahresberichten genannten Fällen identisch sind, konnte nicht festgestellt werden, da der Landesdatenschutzbeauftragte datenschutzrechtliche Bedenken hatte, mir die Aktenzeichen mitzuteilen.

6) IV. Tätigkeitsbericht des Niedersächsischen Datenschutzbeauftragten (1.1. - 31.12.1982) RN 12.8 (= S. 55).

Weiteres einschlägiges Material war nicht zu erhalten. Meine Schreiben an den Datenschutzbeauftragten des Bundes und die der Länder brachten lediglich zwei Bußgeldurteile wegen Verletzung der Meldepflicht nach § 42 I Nr. 4 BDSG. Ansonsten verwiesen mich die meisten kurz lapidar auf die einschlägigen Kommentare und NJW-Fundhefte, denen jedoch nur zwei Verfahren zu entnehmen waren [7]. Ebenfalls ohne auswertbares Material blieb das Anschreiben von siebzehn Datenschutzbeauftragten von Städten und Gemeinden [8].

Schließlich wären so aus dem Zeitraum 1978 - 1982 am Ende 162 Akten für eine Auswertung zur Verfügung gestanden. Da jedoch in einem Fall die Akteneinsicht verwehrt wurde, da eine "Geheimhaltung des Akteninhalts erforderlich" sei, eine Akte unauffindbar war und eine Akte bis zum Abschluß der Auswertung immer "nicht entbehrlich" war, blieben

1 5 9 Akten, die von mir ausgewertet werden konnten.

Bei der Einsichtnahme tauchten nur selten Schwierigkeiten auf, da die erforderlichen Genehmigungen für die Akteneinsicht vorhanden waren. Der Zugang geschah auf folgende Weise: Ein geringer Teil der Akten wurde mir zugesandt, ein anderer Teil einem Lehrstuhl der Universität Tübingen. Der größte Teil der Akten jedoch wurde an den für Datenschutzstrafsachen zuständigen Referenten der Staatsanwaltschaft Stuttgart gesandt, wo sie durchschnittlich ein bis drei Monate zur Verfügung standen. Die erste Akte traf am 4.11.1982, die letzte, die berücksichtigt wurde, am 20.12.1983 ein. Knapp 20 Verfahren mußten vor Ort, bei den jeweiligen Staatsanwaltschaften ausgewertet werden.

7) Es handelt sich um den Fall des LG Bad Kreuznach NJW 1978, 1931 f. und das Urteil des AG Konstanz (= Fall 5 "Vorstandsvorsitzender"; ausführliche Darstellung im Anhang).

8) Der Datenschutzbeauftragte der Stadt Nürnberg hatte mir eine Liste mit 16 Städten, die Datenschutzbeauftragte bestellt hatten, übersandt.

II) Abgrenzung des Untersuchungszeitraumes

Da sich die Untersuchung auf Fälle aus den Jahren 1978 - 1982 beschränken sollte, habe ich die Verfahren nicht in die statistische Auswertung einbezogen, die erst im Jahre 1983 begannen und die mir teilweise von den Staatsanwaltschaften während der im Jahre 1983 andauernden Aktenauswertung zugänglich gemacht wurden. Jedoch werden einige interessante Verfahren in die Darstellung der Fälle einbezogen. In der Auswertung sind dagegen zwei Verfahren enthalten, die 1977 in Rheinland-Pfalz noch unter der Geltung des damaligen Landesdatenschutzgesetzes (LDatG 1974)[9] begannen. Sie wurden einbezogen, da die Strafverfolgungsbehörden auch nach Inkrafttreten des BDSG noch damit befaßt waren:

Beim ersten Verfahren ging es darum, daß ein Einwohnermeldeamt jahrelang die Durchschläge der Neuanmeldungen an die örtliche Kreissparkasse weiterleitete, die dann die "Neubürger" mit einer Werbebroschüre überraschte. Da hier nach Inkrafttreten des BDSG die zunächst gemäß § 170 II StPO mangels Strafantrag eingestellten Ermittlungen wiederaufgenommen wurden, schien mir eine Einbeziehung angebracht.

Das zweite Verfahren ist der wohl bekannteste Fall von Datenschutz-Kriminalität: Es ist der "datenschutzrechtliche Unglücksfall"[10] des LG Bad Kreuznach[11], der mehrfach besprochen wurde[12], weshalb hier auf ein besonders ausführliches Eingehen verzichtet werden kann. Daß das Landgericht in diesem

9) LDatG Rheinland-Pfalz vom 24.1.1974 GVBl. 1974 S. 31 f.

10) Dammann NJW 1978, 1906.

11) LG Bad Kreuznach NJW 1978, 1931 f.

12) Marx DSWR 1979, 86; Dammann NJW 1978, 1906; Gola MDR 1980, 131; Haft NJW 1979, 1195; Ausschuß für Datenschutz des Landes RP, 5. TB, LT-Drs. 8/3492, S. 4; vgl. auch Sieber S. 2/138 FN 85 und DuD 1979, 51.

"undurchdringlichen Dickicht einer Kombination unklarer Begriffe mit einer komplizierten Konstruktion" - wie es Dammann [13] ausdrückt, steckenblieb, ja - wie Haft [14] meint - "glorreich scheiterte" war angesichts der oben dargestellten strukturellen und quantitativen Komplexität [15] nicht verwunderlich [16].

B) Die Methodik der Auswertung

Die Auswahl der Auswertungsmethoden muß mit den Besonderheiten der Fragestellung und des Gegenstandes abgestimmt werden [17]. Erforderlich ist somit eine Orientierung am Auswertungsziel. Das Ziel der Auswertung war, festzustellen, wie sich die komplexe Verweisungstechnik der Datenschutzgesetze in der Praxis auswirkt und welche charakteristischen Fehler dabei auftraten.

I) Wahl der Untersuchungsmethode

Nachdem der Entschluß gefaßt worden war, die Akten der Ermittlungsverfahren zur Datenschutz-Kriminalität zu analysieren [18], lag damit inzidenter als Untersuchungsmethode eine Erhebung mittels Fragebogen fest. Die Fragebogentechnik gehört zum klassischen Instrument wissenschaftlicher Untersuchungen und erfüllt die Forderungen nach einer möglichst hohen Objektivität von Testaufnahme und Testauswertung [19]. Die ursprünglich geplante computermäßige Auswertung der Daten war ein weiteres Argument für die Erstellung eines strukturierten Erhebungsbogens.

13) Dammann NJW 1978, 1907.

14) Haft DSWR 1979, 141.

15) Vgl. nur die Abb. 3.3 "Verweisungsbaum", § 3 B I der Arbeit.

16) So auch der Ausschuß für Datenschutz des Landes Rheinland-Pfalz in seinem 5. TB, LT-Drs. 8/3492 S. 5.

17) Göppinger, Kriminologie, S. 111 (vgl. auch S. 104 ff.).

18) Zu Aktenerhebungen in kriminologischer Sicht: Göppinger S. 112 - 116; zur Auswertung von Kriminalfällen: Middendorf S. 10 - 14 und Berckhauer, Aktenuntersuchung, S. 56 f.; zum grundsätzlichen Problem der Aktenauswertung Steffen S. 89 - 108 und Seibert S. 9 ff.

19) Danzig/Jeschek/Egger S. 28.

Schließlich war durch die Fragebogentechnik die Einbeziehung aller Verfahren des Fünfjahrezeitraumes möglich, so daß sowohl die Gefahr statistischer Zufälligkeiten so gering wie möglich gehalten werden konnte, als auch die Bildung von Kontrollgruppen überflüssig war.

Wie Göppinger indessen ausführt, besteht bei standardisierten Fragebogen mit vorgegebenen Kategorien "die große Gefahr, daß nur noch das gesehen und zugeordnet wird, was im Sinne der vorgegebenen Erhebungsfakten relevant ist, daß man also im Grunde ein Abbild des Erhebungsbogens erhebt" [20]. Um diese Gefahr zu vermeiden, wurde beschlossen, als Erhebungsmethode ein System offener Fragen zu entwickeln, die bliebig differenzierte Antworten zuließen. Ja/Nein-Fragen oder bestimmte Zuordnungskategorien sollten so weit wie möglich ausgeschlossen sein.

II) Gang der Konstruktion des Auswertungsbogens

Die Kriterien der Auswertung mußten selbst entwickelt werden, was bei diesem neuartigen und komplexen Regelungssystem der Datenschutzgesetze besondere Schwierigkeiten bereitete. Nach Danzig/Jeschek/Egger "gehört die Fragebogenkonstruktion zu den diffizilsten Phasen des Untersuchungsganges, da sie zum größten Teil von der Intuition des Forschers abhängig ist" [21].

Die Methode der offenen Fragen erwies sich hier zwar insofern als günstig, als sie vorstrukturierte oder gar vorteilsbehaftete [22] Antworten verhinderte bzw. erschwerte, konnte jedoch nicht die Formulierung der Fragen ersetzen. Außer der Unter-

20) Göppinger, Kriminologie, S. 129/130.

21) Danzig/Jeschek/Egger S. 29; ebenso E. Raab S. 255.

22) Zur Aufhellung von Vorurteilsstrukturen: Haft MDR 1980, 376 f.

suchung von Sieber [23], die sich indessen mit der vermögensorientierten Computerkriminalität befaßt, standen auf diesem Gebiet keine vergleichbaren Untersuchungen zur Verfügung, die Anregungen hätten geben können. So war offensichtlich, daß der einmalige Entwurf eines Kataloges von Prüfungspunkten nicht ausreichen würde, sondern ein mehrstufiges Vorgehen und mehrmaliges Testen nötig war. Auf der anderen Seite waren die einzelnen Akten nur jeweils für einen kurzen Zeitraum und nur an bestimmten Orten verfügbar. Damit bestand nicht die Möglichkeit, zuerst alle Akten durchzuarbeiten und danach die Kriterien zu entwickeln und auszudifferenzieren. Aus diesen vielschichtigen Zwängen heraus wurde deshalb folgende abgestufte Methode angewandt:

Als erstes wurde ein Auswertungsbogen entworfen, der ein sehr grobes und weitmaschiges Netz von Fragen enthielt. Nach der Auswertung der zuerst eingetroffenen zehn Verfahren stellte sich schnell heraus, daß teilweise eine falsche Blickrichtung gewählt worden war und viele Gesichtspunkte einer modifizierten und anders ausdifferenzierten Fassung bedurften. So wurde der Fragebogen überarbeitet und umstrukturiert und ein neuer "Durchlauf" unter Einbeziehung weiterer, inzwischen eingetroffener, Verfahren unternommen. Da indessen die Akten nicht unbegrenzt zur Verfügung standen, mußte nach dem dreißigsten Fall eine Zasür gemacht und der endgültige Auswertungsbogen entworfen werden [24]. Mit seiner Hilfe begann daraufhin die eigentliche Auswertung.

Nachdem alle Fragebogen ausgefüllt waren, wurden die Antworten der offenen Fragen kategorisiert und zu Gruppen zusammengefaßt. Als letzter Schritt wurden Endauswertungslisten gebildet, in die die Ergebnisse der Auswertung und Neugruppierung übertragen wurden, bevor das Zusammenzählen und Analysieren erfolgte.

23) Sieber, Computerkriminalität und Strafrecht, 2. Aufl. 1980.

24) Der Auswertungsbogen ist im Anhang abgedruckt.

III) Arten der Auswertungskriterien

Der Auswertungsbogen enthielt keine scharfe und expressis verbis durchgeführte Trennung in einen verfahrens-, tat- und beschuldigtenbezogenen Komplex, da die einzelnen Fragen oftmals dem einen oder anderen Bereich zugeordnet werden konnten. Aus Gründen der Übersichtlichkeit soll indessen bei einer groben Darstellung der Auswertungskriterien eine solche Einteilung vorgenommen werden.

1) Zum Verfahren könnte man beispielsweise folgende (zusammengezogenen) Fragen rechnen: Wer erstattete wann, bei wem Strafanzeige und wegen welcher Delikte? [25] Lag eine Mitwirkung von Sachverständigen, Datenschutzbeauftragten oder Aufsichtsbehörden vor?

2) Als Charakteristika der verfolgten Tat könnte man die mit den Tatbestandsmerkmalen verbundenen Fragen bezeichnen: Wo waren wie welche Daten gespeichert? Welche Tatmodalitäten lagen vor und wer stellte zu welchem Zeitpunkt Strafantrag? Diese tatbezogene Fragegruppe bildet den Kern der vorliegenden Arbeit, da hier das Problem der verweisungsspezifischen Fehler in der Rechtsanwendung anzusiedeln ist.

3) Schließlich ließ sich ein beschuldigtenbezogender Komplex bilden, in dem nach Alter, Familienstand, Geschlecht, Beruf, Vorstrafen, Motiven für die Tat und Verhältnis zum Opfer gefragt wird.

25) Es wurde davon ausgegangen, daß auch "Nicht-Strafantragsberechtigte" Strafanzeige erstatten. Wie später gezeigt wird, bestätigte dies die Auswertung.

IV) Bildung der Kriterien des Auswertungsbogens

Schon die "Entstehungsgeschichte" des Auswertungsbogens offenbart die Schwierigkeiten, denen die Arbeit ausgesetzt war. Da die Methode letztlich vom Gegenstand determiniert ist, dieser selbst hier aber höchstens in Umrissen erkennbar war, mußte sich am Ende der Auswertung trotz der Verbesserungen nach dem zehnten und dreißigsten Verfahren zwangsläufig ein modifiziertes Bild ergeben. Göppinger [26] legt dar, daß "eine dem Gegenstand angemessene Erhebung von"Tatsachen" ein bestimmtes Wissen um die Wirkungszusammenhänge als Ganzes" voraussetzt, "durch die sich erst die Bedeutung bzw. das Gewicht der Einzeltatsache" ergebe. So kristallisierten sich einerseits Fehleinschätzungen und Versäumnisse der im Fragebogen niedergelegten Konzeption heraus, andererseits wurde offenbar, daß überflüssige und nicht verwertbare Daten erhoben worden waren. Einige dieser in der Arbeit nicht behandelten Daten betrafen die mit der Persönlichkeit des einzelnen Beschuldigten zusammenhängenden Fragen. Die beschuldigtenbezogenen Aussagen erwiesen sich für eine wissenschaftliche Erörterung oft als nicht fundiert und ausreichend genug. Infolgedessen wurde auf die gesonderte und ausführliche Darstellung dieser Ergebnisse ("Beschuldigtenanalyse") zum größten Teil verzichtet.

Bei der Kriteriengestaltung mußten solche gebildet werden, aus denen hervorging, daß die Verweisungskomplexität zu Fehlern in der Rechtsanwendung führte. Dies erwies sich jedoch schwieriger als zunächst erwartet. Anhaltspunkte für verweisungsspezifische Fehler erschlossen sich indessen aus Vermerken und Begründungen in den Abschlußverfügungen oder aus der Art und Zielrichtung der Sachverhaltsaufklärung durch die Staatsanwaltschaften. So konnte ein "Überlesen" von stillschweigenden Verweisungen z. B. angenommen werden, wenn ermittelt wurde, obwohl die übermittelten Daten unzweifelhaft

26) Göppinger, Kriminologie, S. 99/100.

weder in einer Datei gespeichert waren, noch dorthin übermittelt werden sollten. Gleichwohl bestand bei diesen Kriterien die Gefahr einer subjektivistischen Fehleinschätzung meinerseits, die nur durch ein ständiges "Bewußtmachen" und mehrmaliges Überprüfen der gefundenen Ergebnisse gemildert werden konnte.

Schließlich wurde bei der Kriterienbildung auf tatsächlich auftretende Kategorien geachtet, um Anhaltspunkte für bereichsspezifische Probleme zu erhalten. So wurde z. B. bei der Frage, welche Daten vorlagen, nicht einfach danach differenziert, ob personenbezogen oder nicht, sondern auch registriert, welcher Art (z. B. Adresse, Geburtsdatum) die Daten waren.

V) Durchführung der Erhebung, statistische Auswertung und Darstellung der Ergebnisse

Da alle Akten von mir und damit der gleichen Person ausgewertet wurden, war eine individuell unterschiedliche Einschätzung von identischen Sachverhalten weitestgehend ausgeschlossen. Die Dauer der Auswertung einer Akte war von deren Umfang abhängig, der von wenigen Blättern bis zu mehreren Leitz-Ordnern schwankte. Das Ausfüllen der Fragebogen nahm im günstigsten Falle eine halbe Stunde, im ungünstigsten zwei volle Tage in Anspruch.

Die ursprünglich geplante computermäßige Auswertung mußte aus Zeit- und Kostengründen unterbleiben, so daß die 159 Fragebogen von Hand ausgewertet werden mußten. Diese manuelle Auswertung verhinderte zwar eine umfassende Erarbeitung von Korrelationen zwischen verschiedenen Auswertungskriterien, war jedoch für die Zwecke der vorliegenden Arbeit kein grundlegendes Manko. Schon die Summierung von einzelnen Punkten war geeignet, die zur fehlerhaften Rechtsanwendung führende Verweisungstechnik darzulegen. Die Reihenfolge der vorgestellten Auswertungskriterien orientiert sich - wie schon dargelegt - an den einzelnen Tatbestandsmerkmalen des § 41 BDSG.

Bei der sprachlichen Darstellung der Fälle entspricht die Wortwahl weitgehend der der beteiligten Personen und Institutionen. Da die Genehmigungen zur Akteneinsicht immer nur unter der Bedingung, daß eine Identifizierung der Beteiligten nicht möglich ist, erteilt wurden, werden hier zwar Originalfälle vorgestellt, es fehlen aber Identifizierungshinweise wie Ortsangaben oder auch Angabe des staatsanwaltschaftlichen Aktenzeichens, da allein der Name der Staatsanwaltschaft bei zahlreichen Fällen mit dem Risiko einer Reanonymisierung [27] verbunden wäre.

C) Verfahrenscharakteristika

In diesem Abschnitt werden die formalen Eigenheiten und Besonderheiten des vorliegenden Materials dargestellt, damit aus der Art und Qualität der Ermittlungsverfahren Kriterien für die Bewertung verweisungsspezifischer Fehler gewonnen werden können.

Untersucht wurde einerseits, wer der Anzeigenerstatter war und wo und aus welchen Gründen er seine Anzeige aufgab, andererseits wurden die Arten und Gründe der Verfahrensbeendigungen analysiert und die Dauer der einzelnen Ermittlungsverfahren registriert. Schließlich werden Bedeutung und Umfang der Einschaltung von Sachverständigen bei den vorliegenden Verfahren erörtert.

I) Anzeigenerstatter

Untersucht wurde zunächst, wer den Anstoß zu den Ermittlungen gab, d. h. wer den Anzeigenerstatter war. Es sollte festgestellt werden, welches Gewicht dabei einerzeits den Anzeigen der Datenschutzbeauftragten in Bund und Ländern, und andererseits den Betroffenen selbst zukam.

27) Allgemein zur Anonymisierung personenbezogener Daten: Hammerbacher DuD 1982, 284 - 292.

II) Stelle der Anzeigeneinleitung

Untersucht wurde weiter, wo die zu den 143 Verfahren führenden 144 Anzeigen (16 Verfahren begannen ja von Amts wegen s. o.[28]) erstattet wurden. Hierbei standen besonders die Anzahl der bei den Datenschutzbeauftragten in Bund und Ländern eingegangenen Anzeigen im Vordergrund, da ein entsprechendes Verhalten vieler Betroffener erwartet wurde.

Zu bedenken war indessen, daß diese Institution zuerst eine Überprüfung und Klärung des Anzeigensachverhaltes herbeiführen konnte ("Filterwirkung") und somit wahrscheinlich nicht alle bei ihnen eingegangenen Anzeigen weitergeleitet wurden.

Die Auswertung ergab, daß über die Hälfte der Ermittlungsverfahren durch Strafanzeige bei der Staatsanwaltschaft eingeleitet wurden, ein Drittel bei der Polizei und ungefähr zehn Prozent bei sonstigen öffentlichen Stellen. Nicht überraschend ist dabei, daß in allen 17 Fällen, in denen der Betroffene seinen Rechtsanwalt die Anzeige einreichen ließ, dieser sich direkt an die Staatsanwaltschaft wandte. Bemerkenswert ist jedoch, wie sich die 15 Anzeigen an die sonstigen öffentlichen Stellen verteilen:

So wurden 5 Anzeigen bei den Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (vgl. § 30 BDSG) und nur 7 bei den Datenschutzbeauftragten (5 x Land, 2 x Bund) sowie 3 bei anderen Stellen (z. B. Amtsgericht) eingelegt. Da fünf der sieben bei den Datenschutzbeauftragten angezeigten Verfahren mit einer Einstellung endeten, spricht dies zudem für eine geringe "Filterwirkung". Somit läßt sich letztendlich nur eine geringe Bedeutung der Datenschutzbeauftragten im Bereich der Strafverfolgung feststellen.

28) Siehe eben, § 5 C I der Arbeit.

Da in einem Verfahren zwei unabhängig voneinander handelnde Anzeigenerstatter berücksichtigt werden mußten, kommt man auf 160 Einleitungen. Hiervon sind genau 10 % von Polizei oder Staatsanwaltschaft von Amts wegen eingeleitet worden, sei es, daß sich aufgrund anderer, schon begonnener, Verfahren "Datenschutz-Verstöße" herausstellten, sei es aufgrund sonstiger Umstände (so z. B. wenn Adressen in Zeitungsanzeigen zum Verkauf angeboten wurden). Der weit überwiegende Teil, nämlich fast 70 % der Verfahren wurde jedoch vom Betroffenen oder seinem Rechtsanwalt eingeleitet. Hierzu gehören auch die Fälle, in denen die Betroffenen sich zunächst an andere Stellen wandten, denn entscheidend im Rahmen dieser Frage war nur, von wem die Initiative zur Strafverfolgung ausging. Die restlichen knapp 20 % wurden angezeigt von sonstigen öffentlichen Stellen, privaten juristischen Personen oder nicht als Betroffenen anzusehenden Dritten ("natürliche nichtbetroffene Personen"), sowie von sonstigen (z. B. anonym).

Überraschend war, daß nur ein einziges Verfahren aufgrund der Initiative eines Landesbeauftragten für den Datenschutz bei der StA eingeleitet wurde, d. h. nur einmal entdeckte diese Institution selbständig eine mögliche Straftat nach den Datenschutzgesetzen.

Aus Tabelle 4.2 ergibt sich eine Aufschlüsselung der Anzeigenerstatter:

Tabelle 4.2 "Anzeigenerstatter":

Betroffener persönlich	94	=	58,8 %
... über seinen Rechtsanwalt	17	=	10,6 %
Polizei/Staatsanwaltschaft	16	=	10,0 %
sonstige öffentliche Stellen	9	=	5,6 %
private juristische Personen	9	=	5,6 %
natürl. nichtbetroffene Personen	11	=	6,9 %
sonstige Anzeigenerstatter	4	=	2,5 %
	160	=	100,0 %

Die Tabelle 4.3 gibt einen Überblick über die Stelle der Anzeigeneinleitung:

Tabelle 4.3 "Stelle der Anzeigeneinleitung":

Anzeige bei der StA	79	=	54,9 %
Anzeige bei Polizei	50	=	34,7 %
Bei Datenschutzbeauftragten	7	=	4,9 %
Bei Aufsichtsbehörden	5	=	3,5 %
Bei anderen Stellen	3	=	2,1 %
	144	=	100,1 %

III) Grund der Anzeige

Im folgenden wurde analysiert, aus welchen Gründen die 143 Verfahren, die nicht von Amts wegen begannen, eingeleitet wurden. Es sollte erforscht werden, ob und mit welchen Delikten die Datenschutzkriminalität typischerweise auftritt.

Dabei ergab sich, daß bei 129 Verfahren der Verstoß gegen die Datenschutzgesetze bzw. Datenmißbrauch angezeigt und bei 14 Verfahren angebliche Verstöße gegen Delikte anderer (unterschiedlichster) Art vorgetragen wurden. Von den 129 Verfahren wiederum wurden 81 allein "wegen des Datenschutzes" (so oft wörtlich) und 48 zusammen mit anderen Delikten zur Anzeige gebracht.

Graphisch ergibt das die folgende Übersicht:

159 Verfahren
- → 16 Beginn von Amts wegen
- → 143 Anzeigenerstattung
  - → 129 wegen "Verstoß gegen Datenschutz"
    - → 81 allein wegen Datenschutz
    - → 48 mit anderen zusammen
  - → 14 allein wegen anderer Delikte

Schlüsselt man die anderen Vorschriften, die bei den Anzeigen allein oder mit dem "Datenschutz" zusammen genannt wurden ("Begleitdelikte") auf, so ergeben sich, der Häufigkeit nach geordnet, die folgenden Delikte (Mehrfachnennung berücksichtigt) aus der Tabelle 4.4:

Tabelle 4.4 "Begleitdelikte":	
17 mal	Beleidigung
14 mal	Vermögensdelikte
13 mal	Amtsdelikte
8 mal	Unlauterer Wettbewerb
7 mal	Verletzung von Privatgeheimnissen
17 mal	sonstige "Delikte" (vom bloßen Sachverhalt über Ordnungs- und Ordnungswidrigkeitenvorschriften bis zu einzelnen, nicht gesondert erfaßten Straftatbeständen).

Die Datenschutzkriminalität wird damit in etwas über der Hälfte der Verfahren allein wegen angeblichen Verstößen gegen den "Datenschutz" zur Anzeige gebracht. Die übrigen Fälle weisen zum größten Teil einen Bezug zu Delikten auf, die unter den "weiten" Datenschutzbegriff fallen [29].

Im Zusammenhang mit der Frage der typischen Begleitdelikte wurde auch untersucht, ob eine Gewaltanwendung vorlag ("Datenraub"). Jedoch kam es bei den hier vorliegenden 159 Verfahren nur in einem Fall zur Gewaltanwendung, als nämlich ein Karteikasten mit Adressen mitgenommen wurde [30]. Diese nur einmalige Anwendung von Gewalt beweist indessen nicht die fehlende

29) Siehe oben, Einleitung, § 1 der Arbeit.

30) Vgl. im Anhang Fall 38 ("Karteikastenraub").

Relevanz des "Datenraubs". Sie dürfte vielmehr damit zu erklären sein, daß derartige Fälle statistisch unter "Raub" oder "Nötigung" erfaßt werden. Zum einen ist deren Deliktsschlüssel den Polizeibeamten geläufiger [31], zum anderen dürfte auch für den Betroffenen der Aspekt der Gewalt (oder Drohung) im Vordergrund stehen.

IV) Verfahrensbeendigung

Die mit dem Abschluß der Ermittlungsverfahren zusammenhängenden Fragen sind für die Einschätzung der Art des vorliegenden Materials von größter Wichtigkeit. Es wird deshalb dargestellt, wie die Verfahren von den Staatsanwaltschaften abgeschlossen wurden und mit welcher Begründung dies geschah:

Bei 6 Verfahren lagen schon keine zureichenden tatsächlichen Anhaltspunkte für ein Einschreiten vor (§ 152 II StPO). In 123 der 159 Verfahren (= 74,5 %) kam es bezüglich eines jeden Beschuldigten zu einer Einstellung nach § 170 II StPO. Diese hohe Zahl von Einstellungen verdeutlicht, warum bisher von einer"fehlenden Realität der Datenschutzkriminalität" [32] gesprochen werden konnte.

Bei den restlichen 30 Verfahren (mit 52 Beschuldigten) waren in 14 Verfahren nur ein Beschuldigter, ansonsten mehrere Beschuldigte beteiligt. Da es bei den letzteren Verfahren für jeden einzelnen Beschuldigten ein anderer Verfahrensausgang möglich war, wurde für diese 30 Verfahren eine verfahrensbezogene und keine beschuldigtenbezogene Aufteilung gewählt.

31) Bei den Anzeigenformularen ist neben der Tat im Klartext auch noch für die (wesentliche) Deliktsart eine Schlüsselnummer - für Datenschutzdelikte z.B. 7180 - anzugeben.

32) Haft NJW 1979, 1196.

Es wurden drei Gruppen gebildet:

- Einstellung nach §§ 153, 153a StPO,
- Antrag auf Erlaß eines Strafbefehls,
- Antrag auf Eröffnung des Hauptverfahrens.

Es ergab sich folgende, tabellarisch dargestellte, Statistik zur Verfahrensbeendigung:

Tabelle 4.5 "Verfahrensbeendigung":

Kein Einschreiten (§ 152 II StPO):	6	=	3,8 %
Einstellung nach § 170 II StPO:	123	=	77,4 %
Einstellung nach §§ 153, 153a StPO	13	=	8,1 %
Antrag auf Erlaß eines Strafbefehls:	8	=	5,0 %
Antrag auf Eröffnung Hauptverfahren:	9	=	5,7 %
Alle ausgewerteten Verfahren:	159	=	100,1 %

Im folgenden werden alle nicht nach den §§ 152 II, 170 II StPO endenden Verfahren näher klassifiziert und sodann die eingestellten Verfahren einer näheren Analyse unterzogen.

1) Nähere Klassifizierung

Von den 13 Verfahren, die für zumindest einen Beschuldigten mit einer Einstellung nach §§ 152, 153a StPO endeten, wurden

- 5 Verfahren nach § 153 StPO [33],
- 8 Verfahren nach § 153a StPO eingestellt [34].

33) Davon werden vorgestellt (vgl. Fallverzeichnis): Fall 3 ("Einkommenshöhe"), Fall 50 ("Nötigungsversuch"), Fall 51 ("Nebenberuf") und Fall 38 ("Karteikastenraub").

34) Davon werden vorgestellt (vgl. Fallverzeichnis): Fall 58 ("Baukasse"), Fall 12 ("Hellseherin"), Fall 61 ("Doppelhaushälfte"), Fall 62 ("Kontaktaufnahme"), Fall 37 ("Bankauskunft") und Fall 68 ("Handwerkersorgen").

Insgesamt 8 Verfahren (mit zusammen 13 Beschuldigten) schlossen zumindest für einen Beschuldigten mit dem Antrag auf Erlaß eines Strafbefehls:

- Davon waren 5 Verfahren mit je einem Beschuldigten, von denen zwei den Strafbefehl akzeptierten [35] und zwei Einspruch eingelegten [36]. In einem Verfahren zog der Betroffene den Strafantrag gegen die Beschuldigte, nämlich seine Mutter, vor Erlaß des Strafbefehls durch den Richter zurück [37]. Im siebten Verfahren steht eine Entscheidung noch aus [38].

- In einem Verfahren akzeptierte einer der vier Beschuldigten den Strafbefehl, die anderen legten Einspruch ein[40].

In 9 Verfahren wurde Antrag auf Eröffnung des Hauptverfahrens gestellt:

- In 2 Verfahren wurde die Eröffnung abgelehnt [41].

- In 6 Verfahren wurde das Hauptverfahren eröffnet. Davon geschah in drei Fällen [42] die Eröffnung wegen völlig anderer Delikte, da Verstöße gegen die Datenschutzgesetze nach § 154 StPO eingestellt wurden. In den anderen Verfahren wurden (auch) Verstöße gegen das BDSG angeklagt [43].

- In einem Verfahren wurde Mitte 1983 Anklage erhoben. Es wurde Ende Januar 1984 "wegen falscher Verdächtigung u. a." gemäß § 153a StPO vorläufig eingestellt.

35) Fall 1 ("Universitätsoperator") und Fall 25 ("Mikroficheeinsicht").

36) Fall 40 ("Zentralnamenskartei") und Fall 5 ("Vorstandsvorsitzender").

37) Fall 60 ("Erbschaftsstreit").

38) Fall 67 ("Programmdoppelung"); gegen den inzwischen erlassenden Strafbefehl wurde Einspruch eingelegt.

39) Fall 21 ("Mikrofichesfund").

40) Fall 59 ("Nachbarstreitigkeiten").

41) Fall LG Bad Kreuznach NJW 1978, 1906 und Fall 32 ("Bankindiskretion")

42) Davon im Anhang vorgestellt: Fall 64 ("Ehevermittlung").

43) Fall 57 ("Verlobtenfinanzen"); Fall 8 ("Verkehrsunfall") und Fall 26 ("Zeitungsabonnenten").

2) Weitere Analyse (Einstellungsbegründungen)

Angesichts der hohen Einstellungsquote von ungefähr achtzig Prozent war zu fragen, auf welchen Gründen die Einstellungen nach § 170 II StPO (und das Fehlen zureichender tatsächlicher Anhaltspunkte gemäß § 152 II StPO) beruhten und welche Reaktionen ("Beschwerde") erfolgten.

Es werden hier nur die Gründe aufgeschlüsselt, die in den erstmaligen Einstellungsverfügungen (teilweise wurde nach einer Beschwerde das Verfahren wieder aufgenommen) zum Ausdruck gekommen sind.

Ausgangspunkt bildeten die 139 Verfahren, in denen zumindest bei einem Beschuldigten eine Einstellung nach § 170 II StPO erfolgte. Da aber nicht immer eine einheitliche Einstellungsbegründung für ein Verfahren als solches erfolgte, sondern in 9 Verfahren mehrere Beschuldigte mit jeweils unterschiedlichen Einstellungsbegründungen vorlagen, ergaben sich zusätzliche 13 Gründe. Weiterhin war zu berücksichtigen, daß das Fehlen eines "genügenden Anlasses zur Erhebung der öffentlichen Klage" auch in einem Verfahren auf mehreren Gründen beruhen konnte.

Daraus ergibt sich schließlich, daß man bei den 139 Verfahren (mit insgesamt 201 Beschuldigten) 175 "Einstellungsbegründungseinheiten" erhält, die sich wie folgt verteilen:

Tabelle 4.6 "Einstellungsbegründungen":

kein wirksamer Strafantrag	34	=	19,4 %
kein Tatverdacht	29	=	16,6 %
Nicht aufklär- oder beweisbar	29	=	16,6 %
Keine Datei	22	=	12,6 %
Befugt/Berecht. Interesse	18	=	10,3 %
Kein Vorsatz	15	=	8,6 %
Speichern nicht strafbar	9	=	5,1 %
Sonstige Begründungen	19	=	10,9 %
	175	=	100,1 %

3) Reaktionen und Fortgang nach den Einstellungen

Nicht alle Betroffenen akzeptierten die Einstellungen, sondern in 36 Fällen wurde dagegen Beschwerde erhoben:

- In 29 Fällen wurde die Beschwerde verworfen, was zu vier Klagerzwingungsverfahren nach § 172 II 1 StPO führte,
- in 4 Fällen wurde vor einer Entscheidung der Staatsanwaltschaft die Beschwerde zurückgezogen,
- in 2 Fällen wurde Anklage erhoben und
- in einem Fall kam es darauf zur Einstellung nach § 153 I StPO.

V) Verfahrensdauer

Das vorletzte verfahrensbezogene Kriterium war das der Dauer. Zwar war Anfang 1984 der Ausgang von zwei Verfahren noch offen, da diese aber inzwischen alle über zweieinhalb Jahre dauern, konnten sie in der letzten Rubrik (mehr als 30 Monate) erfaßt werden.

In der Tabelle 4.7 wurde die Länge aller Verfahren in absoluten und dann in Prozentzahlen angegeben.

Tabelle 4.7 "Verfahrensdauer":

Dauer Monate	Alle abs.	Alle %
bis 3	46	28,9
3 - 6	40	25,2
6 - 9	26	16,4
9 - 12	20	12,6
12 - 15	10	6,3
15 - 18	7	4,4
18 - 21	2	1,3
21 - 24	2	1,3
24 - 30	3	1,9
und mehr	3	1,9
	159	100,2

Wie die Tabelle zeigt, wurden ungefähr sechzig Prozent der Verfahren innerhalb eines halben Jahres abgeschlossen. Einer der Gründe dürfte in der hohen Einstellungsquote von über achtzig Prozent der Verfahren liegen.

VI) Umfang und Bedeutung von Sachverständigen

Da die Datenschutzkriminalität eng mit der Arbeit automatischer Datenverarbeitungsanlagen verbunden ist, war zu erwarten, daß bei vielen dieser 159 Verfahren Sachverständige aus diesem Bereich eine entscheidende Bedeutung zukommt.

Die Auswertung ergab indessen nur eine geringe Beteiligung, da sie - bei weitester Interpretation des Begriffs - lediglich in zehn Verfahren mitwirkten:

Davon hätte man vier auch unter die Rubrik "sachverständiger Zeuge" einordnen können, denn hier gab das Opfer/der Betroffene bzw. seine Angestellten Auskünfte oder Erläuterungen über die technischen Modalitäten.

In 2 Fällen erläuterten die in diesem Verfahren beschuldigten Behörden der Staatsanwaltschaft und/oder der Polizei Arbeitsablauf und Rechtsgrundlagen ihrer Tätigkeit.

In zwei weiteren Verfahren lagen Gutachten von am Verfahren unbeteiligten Dritten vor:

So einmal von einer Computerherstellungsfirma (es ging um eine technische Frage) und einmal ein Prüfungsbericht eines Landesbeauftragten für den Datenschutz.

Bei den beiden restlichen Verfahren schließlich waren EDV-Spezialisten von Landeskriminalämtern zur Aufklärung herangezogen worden.

Somit hatte die Einschaltung und Mitwirkung von EDV-Sachverständigen nicht die Bedeutung, wie man eigentlich hätte vermuten können. Allerdings dürfte der Grund darin liegen, daß es bei Persönlichkeitsverletzungen mehr um rechtliche als um tatsächliche Fragen geht, während für die Fragen der Computerkriminalität die Aufklärung des Sachverhaltes im Vordergrund stehen dürfte.

§ 5

Auswertung zum Problem des Schutzbereichs der Datenschutzgesetze

Das wichtigste positive Erfordernis für die Anwendung der Datenschutzgesetze ist das Vorliegen einer Datei, weshalb diese Frage im Abschnitt A untersucht werden soll. Daran anschließend sollen die negativen Ausgrenzungen erörtert werden, so daß im Abschnitt B das Problem der internen Daten und das Medienprivileg dargestellt wird.

A) Das Kriterium "Datei" als Anwendungsvoraussetzung

Die Strafbestimmungen des Bundes- und der Landesdatenschutzgesetze verweisen implizit auf den Anwendungsbereich. So sind nur solche personenbezogene Daten geschützt, die "in Dateien gespeichert, geändert, gelöscht oder aus Dateien übermittelt werden" [1]. Die zentralsten und vorrangigsten Auswertungsfragen waren deshalb die mit dem Begriff "Datei" [2] zusammenhängenden Auslegungsprobleme. Der Dateibegriff ist bereits während der Gesetzesberatungen intensiv wie kaum ein anderer diskutiert worden [3] und gehört zu den problematischsten Bestimmungen der Datenschutzgesetze [4].

1) § 1 II BDSG und alle Landesdatenschutzgesetze: § 1 II LDSG BW; Art. 1 II BayDSG; § 3 II BlnDSG; § 1 II BrDSG; § 1 II HmbDSG; § 1 II HDSG; § 2 II LDatG RP; § 1 II SDSG und § 1 I LDSG SH.

2) Er ist in allen Datenschutzgesetzen einheitlich definiert: § 2 III Nr. 3 BDSG; § 4 III Nr. 3 LDSG BW; Art. 5 III Nr. 3 BayDSG; § 4 III Nr. 3 BlnDSG; § 2 III Nr. 3 BrDSG; § 4 IV Nr. 3 HmbDSG; § 2 III Nr. 3 HDSG; § 2 III Nr. 3 NDSG; § 2 III Nr. 3 LDSG NW; § 3 III Nr. 3 LDatG RP; § 3 III Nr. 3 SDSG und § 2 IV Nr. 3 LDSG SH.

3) Auernhammer, Kommentar, § 2 RN 20.

4) Dammann in: Simitis/D/M/R § 2 RN 1974.

I) Die Auslegung des Begriffes "Datei"

In der Literatur war und ist bis heute umstritten, was unter einer "Datei" zu verstehen ist. Der Streit konzentriert sich auf die Frage, ob zwei, drei oder vier Merkmale vorliegen müssen [5], nach denen erfaßt und geordnet und dann umgeordnet und ausgewertet werden kann. Weitere Streitpunkte sind z. B. die Fragen, was ein Merkmal ist [6], ob die Möglichkeit der Auswertung [7] ausreicht, ob auch eine Zwischendatei eine Datei im Sinne des Gesetzes ist [8], sowie, ob die Begriffe der EDV bei der Auslegung zu verwenden sind [9].

Die Rechtsprechung hatte sich nur vereinzelt mit dem Begriff "Datei" zu befassen [10]. Zur Frage der Anzahl der Merkmale ist auf eine Entscheidung des VG München zu verweisen, wonach vier Sortiermerkmale erforderlich sind [11].

5) Vgl. dazu Auernhammer, Kommentar, § 2 RN 25 mwN; für 2 Merkmale: Louis RN 50; für 3 Merkmale: Erlaß des Bundesverteidigungsministeriums, erläutert von Lux in BWV 1979, 276 f.; für 4 Merkmale: Ordemann/Schomerus § 2 Anm. 3.1.1; Dammann in: Simitis/D/M/R § 2 RN 188; Schulz BKK 1978, 59; Gola MDR 1977, 450; Kutzmann Erl. zu § 3 Anm. 5.7.; Schmid Polizeiblatt für Baden-Württemberg 1980, 82; demgegenüber Ruckriegel, Kommentar LDSG NW Erl. 12 zu § 2: "4 nicht zwingend".

6) Vgl. dazu sogleich weiter unten.

7) Vgl. Auernhammer, Kommentar, § 2 RN 24; Ordemann/Schomerus § 2 Anm. 3.3.1.

8) Vgl. Dammann in: Simitis/D/M/R § 2 RN 87; Ordemann/Schomerus § 2 Anm. 2.1; Auernhammer, Kommentar, § 2 RN 24.

9) Dafür, daß der Begriff der Datei nicht im Sinne der EDV-Terminologie, sondern umfassender zu verstehen ist:
Auernhammer, Kommentar, § 2 RN 21; Dammann in: Simitis/D/M/R § 2 RN 176; Gallwas in: Gallwas/S/S § 2 RN 34; Schweinoch/Geiger Erl. 11 zu Art. 5 BayDSG; vgl. auch Ruckriegel Erl. 12. zu § 2 LDSG NW.
Ein völlig anderer Ansatz zur Aufarbeitung der Problematik findet sich bei Ringwald, INPOL und StA, S. 63, 109 ff.: Danach soll das BDSG nur zur Anwendung kommen, wenn nicht der jeweils zu verarbeitende Einzelfall den Informationsfluß bestimmt, die bei einer Stelle zur Verfügung stehenden Daten nicht durch den gerade dort zu erledigenden Einzelvorgang bestimmt sind.

10) Vgl. den Fall OLG München NJW 1982, 244 - 246 = WM 1982, 51 - 54 = DSWR 1982, 32 - 34 und VG München NJW 1981, 475 = DuD 1981, 129; sowie bei FN 24.

11) VG München NJW 1981, 475 = DuD 1981, 129.

In der ersten Auswertungsphase, d. h. bei der vorläufigen Auswertung der ersten dreißig Verfahren [12], wurde deshalb die Anzahl der Merkmale untersucht. Dazu mußte jedoch zuerst geklärt werden, was als "Merkmal" zu verstehen ist.

In der Literatur wird gefordert, daß als Merkmale nur solche Kriterien anzusehen sind, die "für eine sinnvolle Ordnung der Datei notwendig" seien [13], "ungeachtet dessen, daß sich das Merkmal noch in weitere Einzelkriterien auflösen läßt" [14]. Aufbau und Zweckbestimmung der Dateien seien entscheidend [15]. "Ordnungs- und Suchkriterien, die zwar denkbar, aber datenschutzrechtlich irrelevant" seien, seien auszuscheiden [16]. Es sei "von einer natürlichen Betrachtungsweise und von der für den jeweiligen Bereich maßgeblichen Verkehrsanschauung auszugehen" [17].

Gemeinsame Folge dieser Überlegungen ist, daß es über einen modifizierten Dateibegriff zu einer Einschränkung des Anwendungsbereiches des Gesetzes kommt. Doch abgesehen davon, findet diese Interpretation weder im Wortlaut einen Anhaltspunkt, noch im Sinn und Zweck des Gesetzes eine Stütze. Das Argument einer "sinnvollen Ordnung" verkennt, daß die Mißbrauchsgefahr nicht darin besteht, da eine "sinnlose" Ordnung vorliegt, sondern, daß überhaupt eine Strukturierung und somit leichtere

12) Vgl. dazu oben § 4 B der Arbeit.

13) Schulz, BKK 1978, 60.

14) Ordemann/Schomerus § 2 Anm. 3.3.1.

15) Ordemann/Schomerus § 2 Anm. 3.3.1.

16) Gallwas in: Gallwas/S/S § 2 RN 41.

17) Dammann in: Simitis/D/M/R § 2 RN 190 mwN.

Verfügbarkeit vorhanden ist, die für andere als für die ordnungsgemäße Betreibung zunächst vorgesehenen, Zwecke mißbraucht werden kann. Deshalb greift auch die Orientierung an Aufbau und Zweckbestimmung der Datei ins Leere, denn Anknüpfungspunkt muß die Persönlichkeitssphäre des Einzelnen und nicht die Ordnung der Datensammlung sein. Selbst bei einem zweckhaften Aufbau einer Datensammlung können durchaus einige Merkmale als "unzweckhaft" erscheinen, doch sind sie dies dann nur in Bezug auf die funktionsgerichtete Verwendung der Datei. Für einen Täter jedoch können gerade diese "unzweckhaften" Merkmale die entscheidenden und für einen Betroffenen die ihn am stärksten verletzenden sein. Es gibt keine neutralen oder wertfreien Merkmale. Datenschutzrechtlich relevant kann - wie auch das BVerfG im Volkszählungsurteil feststellt [18] - jedes Merkmal werden, wobei diese Entscheidung nicht nur bei der Aufnahme der (elektronischen) Datenverarbeitung und Strukturierung der Datei(en), sondern auch erst im Zeitpunkt der konkreten Anwendung bzw. des Mißbrauchs fallen kann.

Somit ist als Merkmal jede kleinstmögliche Sinneinheit, d. h. jede praktisch verwendbare Informationseinheit, anzusehen [19]. Das führt dazu, daß dann schon Name und Vorname als zwei Merkmale gelten, wenn - was regelmäßig der Fall sein dürfte - aus dem Vornamen auf das Geschlecht geschlossen werden kann [20].

Ausgehend von der Definition des Merkmals als kleinstmögliche Sinneinheit wurden deshalb die ersten dreißig Verfahren daraufhin untersucht, wieviele Merkmale jeweils vorlagen [21].

18) BVerfG NJW 1984, 419, 422 ("unter den Bedingungen der automatischen Datenverarbeitung gibt es kein "belangloses" Datum mehr").

19) Ähnlich Louis RN 51: "Jedes Kriterium, nach dem eine sinnvolle Umgruppierung erfolgen kann"; sowie Ruckriegel, Erl. 12 zu § 2 LDSG NW "jedes zur Ordnung (Umordnung) und Auswertung geeignete Datum oder Zeichen".

20) Im Fall des LG Bad Kreuznach (NJW 1978, 1931 f.) kam es einem der Beschuldigten nur darauf an, Adressen von weiblichen Personen zu erhalten (um seine Aussteuerwaren zu verkaufen).

21) Vgl. dazu oben § 4 B der Arbeit.

Dabei wurde festgestellt, daß die theoretische Erörterung der Frage "wieviele Merkmale sind für das Vorliegen einer Datei nötig", für die Praxis unergiebig ist [22], da in allen Verfahren immer mehr als vier Merkmale vorlagen.

Die bloße Frage: "Liegt eine Datei vor?" mit den einzig möglichen Antworten "Ja/Nein" erwies sich ebenso als zu undifferenziert und hätte zudem eine Festlegung des Dateibegriffes notwendig gemacht. Damit aber hätte die Gefahr bestanden, daß die Auswertung deshalb problematisch und nur beschränkt aussagekräftig gewesen wäre, denn das Ergebnis wäre dann von der Auslegung des Begriffs "Datei" abhängig gewesen. Da aber die Zielsetzung der Arbeit nicht ist, eine eigene Interpretation des Dateibegriffes zu entwickeln und den vielen vorhandenen Meinungen eine neue hinzuzufügen, mußte ein anderer Weg gewählt werden. Es wurde nicht versucht, zuerst den Begriff zu bilden und dann die Fälle darunter zu subsumieren, sondern versucht, die Verfahren zu klassifizieren und dann ausgehend von der Grundlage einer rechtstatsächlichen Einteilung die Fragestellung der Auslegung des Begriffes "Datei" von neuem zu erörtern.

Am zweckmäßigsten erschien mir dabei zunächst eine Einstufung der Verfahren in drei Kategorien, nämlich

erstens in die Fälle, die nach jeder Auslegung unter den Dateibegriff fallen ("EDV-Anlagen"),

zweitens die Fälle, bei denen das Verständnis der Dateidefinition entscheidend ist ("Graubereich") und

drittens die Fälle, die schon nach dem Wortlaut des Gesetzes nicht unter den Dateibegriff fallen ("Nicht-Datei").

22) Dies vermuteten auch schon Schweinoch/Geiger Erl. 14. zu Art. 5 BayDSG; Auernhammer, Kommentar, § 2 RN 25; Bergmann/Möhrle § 2 10.2; Louis RN 50.

Als Oberbegriff für diese drei Kategorien wurde bewußt der Begriff "Speicherort ("Quelle")"gewählt, da er "unbelastet" von jeglichen Auslegungsfragen erschien. Dieser Begriff hat den Vorteil, daß er zum einen keine vorweggenommene Entscheidung für eine Auslegungsvariante beinhaltet und zum anderen rechtstatsächlich und pragmatisch interessante weitere Untergliederungen zuläßt. Gerade die Antworten auf diese "untechnische" Frage ("wo befanden sich die Daten?"), sind geeignet, die theoretischen Auslegungsfragen auf die praktischen Bedürfnisse, d. h. die der Rechtsanwender, zu konzentrieren. Desweiteren ist damit möglich, Anhaltspunkte für kriminalpolitische und bereichsspezifische Überlegungen zu gewinnen. So ist es zwar für die Auslegung des Begriffs "Datei" (zunächst) wenig ergiebig zu wissen, wie oft Daten aus EDV-Anlagen der Polizei, der Sozialversicherungsträger oder privater Unternehmen Ziel der Beschuldigtenaktivitäten waren, für die Schaffung bereichsspezifischer Gesetze (SGB X!) können diese Ergebnisse jedoch Wegweiser für die Ausformung von Gesetzen sein. Für die Frage des Dateibegriffes selbst kann die Einteilung in verschiedene "Speicherorte ("Quellen")" dann als hilfreich angesehen werden, wenn sie Schlußfolgerungen auf die Notwendigkeit des Begriffs schlechthin zuläßt.

II) Auswertung nach Speicherort ("Quelle") der Daten

Bei der Frage des Speicherorts ("Quelle") war entscheidend, "wo" die Daten, auf die ein Beschuldigter zugreifen wollte, zunächst faktisch verfügbar waren.

Nicht relevant war, wo die Daten nach der ersten Ansich- oder Kenntnisnahme endgültig oder zwischengespeichert waren.

Standen dem Täter nachweislich mehrere Informationsquellen zur Verfügung und blieb die konkrete Quelle aus der er seine Daten erlangte ungeklärt, so wurde die "schwerwiegendste" unterstellt, d. h., der Sachverhalt, bei dem am ehesten der Anwendungsbereich der Datenschutzgesetze angenommen werden

konnte. So wurde in diesen Zweifelsfällen (aber auch nur dann!) eine Kartei einer "Nicht-Datei"(z. B. Akten) und eine EDV-Anlage wiederum einer Kartei vorgezogen. Waren jedoch der oder die Speicherorte nicht eingrenzbar, so wurde er als "unbekannt" registriert.

Bei mehreren Tätern wurde nur die Quelle, auf die zugegriffen wurde, erfaßt und nicht auch noch eventuell nachfolgende Zwischenspeicherorte.

Sowohl bei Alleintätern, als auch bei Tätergruppen war es möglich, daß Informationen nachweislich aus zwei oder mehr voneinander unabhängigen Quellen stammten. Sie wurden dann alle einzeln verbucht.

Nicht als eigenständige Gruppe wurde die der "Magnetbänderfälle" gebildet, da es bei diesen 6 Verfahren jeweils darum ging, daß Inhaber oder Mitarbeiter einer EDV-Anlage Bänder kopierten und weiterleiteten und somit die EDV-Anlage als Speicherort gewertet werden konnte.

So kommt man schließlich bei den 159 Verfahren auf 171 Speicherorte, deren Verteilung sich aus Tabelle 5.1 ergibt:

Tabelle 5.1 "Speicherort ("Quelle")":

EDV-Anlagen	61	=	35,7 %
Graubereich	59	=	34,5 %
Nicht-Datei	40	=	23,4 %
Unbekannt	11	=	6,4 %
alle	171	=	100,0 %

Damit waren personenbezogene Daten nur in einem Drittel der Ermittlungsverfahren, die unter der Rubrik "Verstöße gegen das Bundes- (oder Landes-) Datenschutzgesetz" registriert sind, in EDV-Anlagen gespeichert. Wenn damit umgekehrt bei einem Drittel der Verfahren der Dateibegriff problematisch ist und ein weiteres Drittel gar nicht darunterfallen dürfte, so belegt dies die These eines "weiten" Datenschutzbegriffes der öffentlichen Meinung [23].

Da die Datenschutzgesetze zwischen öffentlichem und nicht-öffentlichem ("privatem") Bereich differenzieren, wurden die 160 bekannten Speicherorte nach Zugehörigkeit zum privaten oder öffentlichen Bereich unterteilt, denn für den privaten Bereich gilt grundsätzlich nur das BDSG. Das Ergebnis ergibt sich aus Tabelle 5.2:

Tabelle 5.2 "Speicherortbereiche":

	gesamt	=	priv.	+	öffentl.
EDV-Anlagen	61	=	33	+	28
Graubereich	59	=	28	+	31
Nicht-Datei	40	=	22	+	18
alle	160	=	83	+	77

Ausgehend von der oben begründeten Einteilung in die Gruppen EDV-Anlagen - Graubereich - Nicht-Datei, soll gesondert die Behandlung durch die Staatsanwaltschaften erfolgen:

23) Vgl. oben § 1 (Einleitung).

III) Gruppe "Nicht-Datei"

Auffallenderweise fallen von den 160 bekannten Speicherorten vierzig, und damit ein Viertel, unzweideutig nicht unter den Dateibegriff im Sinne des § 2 III Nr. 3 BDSG. Da in der Auswertung unter der Gruppe "Nicht-Datei" nur die ganz eindeutig nicht vom Dateibegriff erfaßten Fälle registriert wurden (zumeist handelte es sich um Akten), überraschte dieses Ergebnis. Der Grund dürfte wahrscheinlich in der Überzeugung der Allgemeinheit und damit auch der Anzeigenerstatter liegen, "das Datenschutzgesetz" habe eine neue Rechtslage auch für die bisherigen Bereiche des Umgangs mit personenbezogenen Daten (und das waren vorweigend Akten) geschaffen. Ein weiteres Indiz für diese Überlegung ist die relativ hohe Zahl von klarstellender Rechtssprechung zum Merkmal "Datei" [24]. Sie zeigt die um die Grenzen des Anwendungsbereichs des BDSG (und der Landesdatenschutzgesetze) herrschende Verwirrung. So überrascht nicht, daß auch viele Staatsanwälte hier Schwierigkeiten hatten: Bei den 40 Fällen ganz offensichtlicher "Nicht-Dateien" wurde dies nur in genau der Hälfte der Fälle von den Staatsanwaltschaften erkannt.

Der eigentliche Grund für den Fehler dürfte im übermäßigen und verschachtelten Verweisungssystem zu suchen sein. Die sich aus der Formulierung des § 41 BDSG "... geschützte ... Daten ... " ergebende stillschweigende Verweisung auf § 1 II, III BDSG und die dann davon ausgehenden Weiterverweisungen werden schlicht und einfach übersehen. Genau diesen Fehler machte ja auch das LG Bad Kreuznach [25]. Aber obwohl Dammann [26] in der Besprechung bereits Anfang 1978 darauf hingewiesen und Schweizer [27] bereits Anfang 1977 generell darauf aufmerksam gemacht hatte, es werde oft übersehen, daß eine Datei nötig sei, kam dieser Fehler 20-mal vor.

24) BGH NJW 1981, 1733 = MDR 1981, 1009 = DuD 1981, 204; OLG Frankfurt MDR 1982, 230 = VersR 1981, 1070; OVG Koblenz NJW 1981, 837, 838; VG München NJW 1981, 475; VG Wiesbaden DVBl 1981, 790; LAG Frankfurt ARSt 1983, 124 = DANA 5/1983 S. 11; LAG Köln DB 1983, 1664.

25) LG Bad Kreuznach NJW 1978, 1931 f.

26) Dammann NJW 1978, 1907.

27) Schweizer DB 1977, 292.

Bedauerlicherweise führten zwei dieser "Datei-Unfälle" zu einer gewissen Bemakelung - resultierend aus Fehlverfügungen - des Betroffenen:

So hatte im Fall 3 ("Einkommenshöhe") [28] der Arbeitgeber des Anzeigenerstatters die nachträglich berichtigte Höhe des Einkommens dessen geschiedenen Ehefrau mitgeteilt. Statt jedoch den Arbeitgeber freizusprechen, da die Daten nur aus Akten stammten, wurde das Verfahren "wegen geringer Schuld" gemäß § 153 I StPO eingestellt.

Schwerwiegender ist Fall 4 ("Taxifahrer") [29], in dem der Beschuldigte nichts anderes getan hatte, als eine Adresse für Werbezwecke zu mißbrauchen. Obwohl hier Name und Anschrift weder in einer Datei gespeichert waren, noch daraus übermittelt worden waren, ermittelte die Staatsanwaltschaft gegen ihn. Nach einer Zahlung von 500,-- DM wurde das Verfahren schließlich gemäß § 153 a StPO eingestellt.

IV) Gruppe "EDV-ANLAGEN"

EDV-Anlagen waren in 61 Fällen (= 35,7 %) als Speicherorte der Daten auszumachen [30]. Soweit sie betroffen waren, konnte von einer Datei im Sinne der Datenschutzgesetze ausgegangen werden. Die Probleme lagen hier nicht bei der Frage, ob die Datenschutzgesetze anwendbar sind. Vielmehr war zu untersuchen, welches Datenschutzgesetz, das des Bundes oder das des jeweiligen Landes, einschlägig war. Dabei sollte festgestellt werden, inwieweit die in § 7 II BDSG statuierte Verweisung auf die Landesdatenschutzgesetze, sowie die in § 79 III 1 SGB X normierte Ausnahme zur Ausnahme des § 7 II BDSG, gesehen wurde [31].

28) Der Fall ist ausführlich im Anhang ausgedruckt.

29) Der ausführliche Fall ist im Anhang ausgedruckt.

30) Vgl. oben die Tabelle 5.1 "Speicherort ("Quelle")", § 5 A II.

31) Zum SGB X vgl. die Ausführungen oben, § 3 C der Arbeit. Einen Überblick über die Landesdatenschutzgesetze gibt Gola MDR 1980, 181 und ders. NJW 1982, 1498. Siehe auch NJW 1981, 1482.

Zunächst jedoch soll die oben angesprochene rechtstatsächliche Einteilung [32] der EDV-Anlagen erfolgen, um zu zeigen, welche Bereiche in der Praxis das Ziel der Beschuldigtenaktivitäten darstellten. Das Ergebnis zeigt Tabelle 5.3:

Tabelle 5.3 "EDV-Anlagen-Verteilung":

EDV, privat, eigen	10	=	16,4 %
EDV, privat, Auftrag	6	=	9,8 %
EDV, privat, Auskunftei	17	=	27,9 %
EDV, Sozialbereich	6	=	9,8 %
EDV, Polizei	10	=	16,4 %
EDV, sonst. öffentlich	12	=	19,7 %
	61	=	100,0 %

Erläuterungen zur Tabelle 5.3 "EDV-Anlagen-Verteilung":

EDV, privat, eigen:

Es handelt sich um Unternehmen der Privatwirtschaft ("nicht-öffentliche Stellen") mit eigenen Datenverarbeitungsanlagen.

EDV, privat, Auftrag:

Hierunter werden private Service-Unternehmen verstanden, deren alleinige Tätigkeit darin besteht, für andere Unternehmen Rechnerleistungen zu erbringen.

32) Vgl. oben, § 5 A I der Arbeit.

EDV, privat, Auskunftei:

Bei den in dieser Rubrik verbuchten Fällen befanden sich die Daten in EDV-Anlagen von Auskunfteien [33]. Ihr Aufgabenkreis ist dem der Detekteien verwandt, nur liegt der Schwerpunkt bei den Auskunfteien bei der geschäftlichen Auskunftserteilung [34]. Die betriebstypische Leistung läßt sich schlagwortartig als Information über die Kreditwürdigkeit und Kreditfähigkeit umreißen [35].

EDV, Sozialbereich:

Darunter fallen Anstalten und Körperschaften des öffentlichen Rechts, die in dem Bereich der staatlichen Daseinsfürsorge tätig sind, der sich mit der sozialen Sicherung befaßt und in deren Anlagen sich medizinische (iwS) Daten befinden.

EDV, Polizei:

Hierunter werden die polizeilichen Datenverarbeitungsanlagen der Länder und des Bundes zusammengefaßt [36].

EDV, sonst. öffentl.:

Alle in den öffentlichrechtlichen Bereich fallenden Anlagen, die nicht zur Polizei oder zum Sozialbereich gehören (z. B. Uni- und kommunale Rechenzentren).

33) Zu den Auskunfteien: Neumann S. 44 ff. und Gerth DuD 1983, 12 ff. Zu den Handelsauskunfteien: O. Mallmann, Zielfunktionen, S. 80 ff.; Neumann S. 21 und 57. Speziell zur Creditreform: Meister, Datenschutz, S. 60 ff.; zu den Detekteien: Meister, Datenschutz, S. 72 f. Zur Arbeit der SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung): Ungnade, Zeitschrift für das gesamte Kreditwesen 1979, 57/58; Peitzsch DSWR 1980, 33 f.; Simon DANA 1/1982 S. 18; Meister, Datenschutz, S. 58 f.; O. Mallmann, Zielfunktionen, S.94 ff.; Louis RN 166, 167; Höfer/Kaspari S. 163 - 186; Neumann S. 22 und Voss DuD 1979, 183 - 189.

34) Nach Simon DANA 1/1982 S. 18, waren es 1975 allein von den Handelsauskunfteien jährlich ca. 20 Mio. Auskünfte.

35) Neumann S. 21.

36) Zum polizeilichen Verbundsystem INPOL findet sich eine ausführliche Darstellung bei Ringwald, INPOL und StA, § 1 (S. 23 - 39).

Das BDSG umfaßt sowohl die Datenverarbeitung nicht-öffentlicher Stellen, wie auch die von Behörden und sonstigen öffentlichen Stellen. Bei der letzten Kategorie jedoch gemäß § 7 II BDSG grundsätzlich nur "soweit der Datenschutz nicht durch Landesgesetz geregelt ist". Somit sind die Anwendungsbereiche von Bundes- und Landesdatenschutzgesetz nur in Bezug auf die Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen abzugrenzen. Die Aufgliederung in Tabelle 5.3 zeigt nun, daß bei den drei letzten Gruppen diese Abgrenzung vorzunehmen war, wobei die seit dem 1.1.1981 geltende Rechtsänderung durch das SGB X und die unterschiedlich in Kraft getretenen Landesdatenschutzgesetze zu beachten waren [37]. Faßt man die Ergebnisse aller 61 Verfahren zusammen, so ergab sich in 40 Fällen die Anwendbarkeit des BDSG und in 21 Fällen die des jeweiligen Landesdatenschutzgesetzes. Dieser objektiven Lage wurde die Beurteilung durch die Staatsanwaltschaften gegenübergestellt und in Tabelle 5.4 festgehalten:

Tabelle 5.4 "StA und EDV-Anlagen":

Objektive Lage:	Behandlung durch StA:
BDSG: 40	35 x BDSG 0 x LDSG 5 x offen/beide
LDSG: 21	10 x LDSG 6 x BDSG 5 x offen/beide

37) Siehe FN 31.

In sechs Verfahren wurde also ein "falsches" Datenschutzgesetz angewandt, wobei in allen Fällen vom BDSG anstatt vom jeweiligen Landesdatenschutzgesetz ausgegangen worden war. Die Staatsanwaltschaften übersahen hier wohl § 7 II BDSG, der ausdrücklich auf die Landesgesetze verweist.

Bei zwei dieser Verfahren war zur Tatzeit § 79 III SGB X noch nicht in Kraft [38], womit die Landesdatenschutzgesetze einschlägig gewesen wären. Strafverfolgungsbehörden und Gericht prüften indessen die Strafnorm des Bundesdatenschutzgesetzes.

Fall 5 ("Vorstandsvorsitzender"): [39]

Der Angeklagte hatte eingeräumt, Daten weitergegeben zu haben, die "teils aus den bei der AOK geführten Karteien, teils aus gespeicherten Datenträgern entnommen und auf einem DIN A 4-Blatt zusammengestellt" waren. Das Gerichtsah darin auch einen Verstoß gegen § 41 BDSG und führte aus: "Hierbei spielt es keine Rolle, ob die übermittelten Daten aus einem für die automatisierte Datenverarbeitung benutzbaren Datenträger (Lochkarten, Magnetband, Magnetplatte) oder aus losen Karteikarten, wie sie bei der konventionellen Datenverarbeitung benutzt werden, stammten. Für die Geltung des BDSG ist es unerheblich, in welchem Verfahren personenbezogene Daten verarbeitet werden, ob automatisch oder manuell. Der Begriff der Datei im Sinne des BDSG ist somit wesentlich weiter als er in der Terminologie der Informatik üblicherweise verstanden wird. Er setzt lediglich voraus, daß die Sammlung der Daten nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmalen geordnet und ausgewertet werden kann."

Fall 6 ("Abschiedsabruf"):

Ein ehemaliger Angestellter eines Sozialversicherungsträgers soll vor seinem Ausscheiden Adressen abgerufen haben, um diese dann für seine eigene Vertretertätigkeit zu verwenden. Das Verfahren wurde "wegen Verstoßes gegen das BDSG" mangels Aufklärbarkeit nach § 170 II StPO eingestellt.

38) Es trat am 1.1.1981 in Kraft.

39) Der Fall findet sich ausführlicher im Anhang.

Auch in den übrigen vier Verfahren ermittelten die Staatsanwaltschaften nach § 41 BDSG, wiewohl die Anwendung der entsprechenden Landesstrafnormen geboten war. Dies ist um so erstaunlicher, als in zwei dieser Verfahren (Fälle 7 und 8) die Anzeigenerstatter expressis verbis vom Landesdatenschutzgesetz sprachen und in einem weiteren (Fall 9) der Hinweis zu finden war, der Beschuldigte sei auf die Wahrung des Datengeheimnisses nach dem Landesdatenschutzgesetz verpflichtet worden.

Fall 7 ("Motorradzulassung"): [40]

Eine Kfz-Zulassungsstelle hatte einer Stadt Auskunft erteilt über die Zulassung eines privaten Motorrades eines Stadtbediensteten. Da der Betroffene seinen Strafantrag zurückzog, wurde das Verfahren deshalb eingestellt.

Fall 8 ("Verkehrsunfall"): [41]

Der Beschuldigte hatte eine Kfz-Zulassungsstelle veranlaßt, Daten an ihn weiterzugeben. Der Anzeigenerstatter hatte deshalb Strafantrag wegen Verletzung des Landesdatenschutzgesetzes gestellt. Die Staatsanwaltschaft indessen erhob Anklage wegen Verstoßes gegen § 41 BDSG. Da der Strafantrag nach Anklageerhebung zurückgezogen worden war, erfolgte eine Einstellung des Verfahrens gemäß § 206 a StPO.

Fall 9 ("Zusammenarbeit"):

Ein ehemaliger Angestellter beschuldigte seine frühere Firma, sie arbeite illegal mit einem Polizeibeamten zusammen und veranlasse diesen zum Datenabruf. Das Verfahren wurde mangels Aufklärbarkeit gemäß § 170 II StPO eingestellt.

Fall 10 ("Jugendstrafe"): [42]

Eine bei der Polizei beschäftigte Sekretärin wurde beschuldigt, Daten abgerufen zu haben. Das Verfahren wurde wegen verspätet gestelltem Strafantrag eingestellt.

40) Der ausführliche Fall ist in § 6 bei der Frage der personenbezogenen Daten dargestellt.

41) Ausführliche Falldarstellung im Anhang.

42) Ausführliche Falldarstellung im Anhang.

In zehn Verfahren wurde die Entscheidung zwischen den beiden Gesetzen offen gelassen, wobei entweder nur "das Datenschutzgesetz" bemüht wurde, oder aber beide Gesetze kommentarlos angeschnitten wurden, wie z. B. im folgenden Verfahren:

Fall 11 ("Versicherungsverlauf"):

Die Sozialamtsrätin S wurde von ihrem Bruder beschuldigt, bei anderen Behörden Sozialdaten über ihn abgerufen zu haben. Die Anstellungsbehörde der S erklärte, die von S vorgenommenen Anfragen seien vor Erledigung zurückgenommen worden, so daß kein strafbares Verhalten vorliege. Weder nach dem Landesdatenschutzgesetz noch nach dem SGB X in Verbindung mit § 41 BDSG werde der versuchte Abruf bestraft. Die Staatsanwaltschaft stellte das Verfahren (ohne jegliche Nennung von Paragraphen oder Gesetzen) ein, da ein rechtzeitiger Strafantrag fehle. Das durch ein Klagezwingungsverfahren eingeschaltete OLG stellte fest, daß allenfalls ein versuchter Abruf vorliege, der aber weder nach dem Landes- noch dem Bundesdatenschutzgesetz strafbar sei. Im übrigen fehle ein rechtzeitiger Strafantrag.

In der überwiegenden Anzahl der Verfahren (45 Fälle) wurde von den Staatsanwaltschaften das "richtige" Datenschutzgesetz angewandt. Offen bleiben mußte aber, ob dies mehr Zufall oder Folge bewußten Nachvollzugs von Verweisungen war. Problematisch konnten insoweit von vornherein nur die 28 Fälle mit Datenverarbeitung von Behörden oder sonstigen öffentlichen Stellen werden, da grundsätzlich nur hier der Verweis des § 7 II BDSG auf die Landesdatenschutzgesetze gilt. Nur in diesen Fällen konnte sich die Unkenntnis eines Landesdatenschutzgesetzes auswirken. Waren allerdings Stellen betroffen, die zudem unter das Sozialgesetzbuch fielen, so konnte sowohl die mangelnde Kenntnis eines Landesgesetzes, als auch das Sozialgesetzbuches, nicht zur Anwendung eines "falschen" Gesetzes führen, da § 79 III 1 SGB X die Ausnahmeregelung des § 7 II BDSG wieder aufhebt.

Zusammenfassend läßt sich feststellen, daß die Subsidiaritätsregel des § 7 II BDSG nicht nur rechtsdogmatisch problematisch [43]

43) Nach Dammann, NJW 1978, 1907, gerät die Rechtseinheit durch § 7 II BDSG in Gefahr. Vgl. auch oben § 3 der Arbeit.

und zu schwer nachzuvollziehenden theoretischen Angrenzungen, sondern in der Praxis auch zu Fehlern führt. Diese wiegen trotz der gleichen Strafdrohung umso schwerer, als es in zwei der sechs "Fehlverfügungen" zu Anklagen kam [44].

V) Gruppe "GRAUBEREICH"

Unter der Gruppe "Graubereich", die 59 Verfahren umfaßt [45], wurden all die Fälle registriert, bei denen das Vorliegen einer Datei umstritten bzw. von den genauen Umständen des Einzelfalls abhängig war. Ein Indiz für die Probleme dieser Gruppe kann in der längeren Verfahrensbearbeitung gesehen werden. So gehörten von den 27 Verfahren, die über ein Jahr dauerten, überdurchschnittlich viele, nämlich zwei Drittel, zum "Graubereich".

Innerhalb der Gruppe läßt sich eine weitere, am Speichermedium orientierte, Untergliederung in "Karteien", "Listen", "Mikrofilme und Mikrofiches" sowie "Computerausdrucke" vornehmen, deren genaue Verteilung Tabelle 5.5 verdeutlicht:

Tabelle 5.5 "Graubereich":

1) Karteien	39	=	66,1 %
2) Listen	6	=	10,2 %
3) Mikrofiche/-film	6	=	10,2 %
4) Computerausdrucke	8	=	13,6 %
	59	=	100,1 %

44) Es sind die bereits vorgestellten Fälle 5 ("Vorstandsvorsitzender") und 8 ("Verkehrsunfall"). Beide Fälle finden sich in ausführlicher Fassung im Anhang.

45) Siehe oben die Tabelle 5.1 "Speicherort ("Quelle")", § 5 A II.

Ausgehend hiervon soll die Dateieigenschaft erörtert und die Behandlung durch die Staatsanwaltschaften dargestellt werden. Dabei ist vorweg festzuhalten, daß in dreizehn der vorliegenden 59 Verfahren Strafrichter beteiligt waren. Es handelt sich um drei Verfahren mit einer Einstellung nach § 153 StPO [46] und vier mit einer nach § 152a StPO [47], sowie einen Strafbefehl [48] und fünf Anklagen mit darauf folgenden Hauptverhandlungen [49]. Besonders anhand dieser Fälle werden die oben gebildeten Untergruppen näher analysiert.

1) KARTEIEN

Die umfangreichste Untergruppe in der Gruppe "Graubereich" stellen die Karteien dar. Erfaßt wurden darunter die unterschiedlichsten praktischen Ausprägungen dieses Speichermediums, von der DIN A 6 Karteikarte bis zu großformatigen Registern. Ihre Gemeinsamkeit besteht in der einheitlichen und gleichartigen Anordnung der einzelnen Aufbauelemente, so daß eine Umordnung und Auswertung möglich ist. Eine Sammlung derartiger Karteikarten wird in der ganz überwiegenden Literatur als Datei im Sinne der Datenschutzgesetze angesehen [50].

46) Fälle 50 ("Nötigungsversuch"), 38 ("Karteikastenraub") und 68 ("Handwerkersorgen").

47) Fälle 12 ("Hellseherin"), 61 ("Doppelhaushälfte"), 62 ("Kontaktaufnahme") und 13 ("Betriebsrat").

48) Fall 25 ("Mikroficheeinsicht").

49) Fälle 40 ("Zentralnamenskartei"), 21 ("Mikrofichefund"), 59 ("Nachbarstreitigkeiten"), 5 ("Vorstandsvorsitzender") und 26 ("Zeitungsabonnenten").

50) Ordemann/Schomerus § 2 Anm. 3.3.1; Dammann in: Simitis/D/M/R § 2 RN 193; Auernhammer, Kommentar, § 2 RN 23; Bergmann/Möhrle Anm. 10.4. zu § 2; Kutzmann Erl. Nr. 5.7. zu § 3 LDat RP; Grell RN 32 zu § 4 LDSG BW; Bautsch Anm. 2 zu § 2 NDSG; Suppes Anm. 10 zu § 2 HDSG; Schweinoch/Geiger Anm. 11 und 13 zu Art. 5 BayDSG; Lücke NJW 1983, 1408; wohl auch Gallwas in: Gallwas/S/S § 2 RN 17; Peitzsch DSWR 1980, 31.
Ohne Begründung: Bull FuR 1979, 397; Hümmerich DVR 1977, 130; Tubies DuD 1979, 158; Louis RN 49; Gola MDR 1977, 450; Ziegler-Jung, Datenschutzfragen, S. 480;
bezügl. ärztl. Karteikarten: Lilie S. 157 und Leib ÖVD 1978, 23; Schulz BKK 1978, 57: Karteien von Betriebskrankenkassen sind regelmäßig Dateien. Schedl Erl. zu § 2 (S. 23): Nur "Kartei", die durch Lochmarkierungen die unterschiedlichen Dateninhalte kennzeichnet". A. A. wohl (allerdings ohne Begründung) Kröger, Einführung C. I. (S. 12).

Auch in der Rechtsprechung wird einer Kartei die Dateieigenschaft zugebilligt. So ist insbesondere auf die Entscheidung des OLG München hinzuweisen [51]:

Fall OLG München:

Bestimmte personenbezogene Daten des Klägers waren in der Kartei einer privaten Kreditschutzorganisation (Beklagte) gespeichert, und er verlangte deshalb Löschung. Das OLG verwandte die Begriffe Kartei und (private) Datei synonym und wandte wie selbstverständlich die Vorschriften des BDSG an, weshalb davon ausgegangen werden kann, daß nach Meinung des Senats auch eine Kartei unter den Dateibegriff des § 1 III Nr. 3 BDSG fällt. Im übrigen wies das Gericht darauf hin, daß die Löschungspflicht des § 915 II ZPO nicht analog auf die in privaten Dateien gespeicherten Daten angewandt werden könne.

Aus den hier vorliegenden Verfahren ist der bereits oben vorgestellte Fall 5 ("Vorstandsvorsitzender") zu nennen, in welchem das Gericht von einem Dateibegriff ausgegangen ist, der auch eine Sammlung von Karteikarten umfaßt [52].

Zuzustimmen ist der in der ganz überwiegenden Literatur und Rechtsprechung vorherrschenden Ansicht, eine Kartei sei als Datei im Sinne der Datenschutzgesetze zu qualifizieren [53]. Der Gesetzgeber wollte - wie aus der Gesetzesbegründung hervorgeht - mit dem Dateibegriff nur erreichen, "daß etwa in Notizbüchern, Akten, Büchern und dergl. gespeicherte Daten nicht unter das Gesetz fallen" [54]. Ferner sollte damit eine Umgehung des Gesetzes verhindert werden [55]. Entscheidender

51) OLG München NJW 1982, 244 - 246 = MDR 1982, 51 - 54. Nach dem BayObLG NStZ 1981, 305 f. fällt ein Eheanbahnungsinstitut, das anhand einer Kartei die Vermittlung durchführt unter den 3. Abschnitt (§§ 22 ff.) des BDSG.

52) Siehe oben, § 5 A IV. Ausführlich im Anhang.

53) Siehe FN 50 - 52.

54) BT-Drs. 7/1027 vom 21.9.1973 S. 18.

55) BT-Drs. 7/1027 S. 17.

Grund für die Einbeziehung von Karteien ist jedoch, daß von einerumfangreichen und sorgfältig angelegten Kartei grundsätzlich die gleichen Gefahren für die Privatsphäre ausgehen, wie von einer EDV-Anlage [56].

Die Staatsanwaltschaften waren außer in dem eben erwähnten Fall 5 in 38 weiteren Verfahren mit der Strafbarkeit im Zusammenhang mit Karteien befaßt. Bevor die Handhabung durch die Staatsanwaltschaften näher erörtert wird, werden die 39 "Kartei-Fälle" aus Gründen der Übersichtlichkeit in zwei Gruppen eingeteilt. Zunächst werden die 21 Verfahren analysiert, in denen eine nicht-öffentliche Stelle im Sinne der Datenschutzgesetze betroffen war [57], sodann die Verfahren, in denen die 18 Karteien bei Behörden oder sonstigen öffentlichen Stellen zu finden waren [58].

a) Karteien nicht-öffentlicher Stellen

Von den 21 Karteien nicht-öffentlicher Stellen sind allein 18 den Auskunfteien [59] zuzurechnen und bedürfen einer gesonderten Betrachtung. Zum einen stellen sie den quantitativ größten Teil aller Karteien überhaupt (46 %) [60], zum anderen fand sich bei den Ermittlungsverfahren in den ersten Jahren der Geltung des BDSG häufig der Einwand der Auskunfteien, die nicht mit EDV-Anlagen arbeiteten, sie fielen nicht unter das BDSG [61]. Da aus der Be-

56) Ähnlich die Gesetzesbegründung (BT-Drs. 7/1027, S. 17) in der ausgeführt wird, "daß der Bürger durch die herkömmliche Form der Datenverarbeitung ebenfalls erheblich in seiner Privatsphäre beeinträchtigt werden kann". A. A. Ringwald, INPOL und StA, S. 109 ff.

57) Hier gilt der 3. und 4. Abschnitt des BDSG.

58) Es gelten hier der 2. Abschnitt des BDSG bzw. die jeweiligen Landesdatenschutzgesetze.

59) Zu den Auskunfteien siehe oben die Erläuterung zu Tabelle 5.3 "EDV-Anlagen-Verteilung", § 5 A IV, sowie dort FN 33 - 35.

60) Vgl. Tabelle 5.5 "Graubereich", wonach insgesamt 39 Kartei-Fälle zu verzeichnen waren (§ 5 A V der Arbeit).

61) Dies wird bestätigt durch die Erfahrungen von Dammann NJW 1978, 1906; Lindemann DuD 1979, 221 und Peitzsch DSWR 1980, 31. Aus den hier vorliegenden Verfahren sei auf die ausführliche Sachverhaltsdarstellung von Fall 12 ("Hellseherin") im Anhang verwiesen.

gründung zum Gesetzesentwurf der Bundesregierung eindeutig der Wille hervorging, die Auskunfteien in den Geltungsbereich des BDSG mit einzubeziehen [62], überraschte dieser Einwand. Wenn man davon ausgeht, daß Auskunfteien für alle recherchierten Privatpersonen Karteikarten anlegen, die systematisch aufgebaut sind, so folgt die Einbeziehung der Auskunfteien aus dem Dateicharakter ihrer Karteien [63]. Eine andere Begründung für die Einbeziehung gab die Staatsanwaltschaft im folgenden Verfahren:

Fall 12 ("Hellseherin"): [64]

Die Auskünfte, die die beschuldigte Handelsauskunftei erteilt, sind jeweils immer nach dem gleichen Schema gegliedert. So heißt es in der Anleitung für die Mitarbeiter der Auskunftei unter der Rubrik "Gliederung der Auskünfte über Privatpersonen und freie Berufe":

"Jede Auskunft über Privatpersonen besteht aus:
a) Persönliches,
b) Beurteilung,
c) Tätigkeit,
d) Einkommen,
e) Grundeigentum,
f) sonstiges Vermögen,
g) Zahlungsweise,
h) eventl. Bankverbindung,
i) Redaktionszeile,
j) Kredit- und Sonderfragenbeantwortung."

Die Staatsanwaltschaft sah nun diesen "Auskunftsspiegel" als Datei an und bejahte so die Anwendbarkeit des BDSG.

Dieser Qualifizierung des "Auskunftsspiegels" als Datei ist zuzustimmen, da er wie eine Kartei eine einheitliche und gleichartige Struktur der Aufbauelemente aufweist. Er stellt eine großformatige Karteikarte dar und eine Sammlung derartiger Bogen ist folglich als Datei im Sinne der Datenschutzgesetze zu bewerten. Allerdings dürfte es zweckmäßiger sein, auf die bei den Auskunfteien vorhandenen "richtigen" Karteikarten abzustellen, da es

62) BT-Drs. 7/1027 vom 21.9.1973 S. 17 und S. 29.

63) Neumann S. 113; vgl. auch Mallmann in: Simitis/D/M/R § 32 RN 17; Auernhammer, Kommentar, § 31 RN 4 und Ordemann/Schomerus § 31 Anm. 1.1.

64) Die ausführliche Falldarstellung ist im Anhang abgedruckt. Dort werden auch die Einzelheiten des "Auskunftsspiegels" dargestellt. Vgl. auch BGH NJW 1984, 1886 mit Anm. Fiedler JZ 1984, 678.

möglich ist, daß der mit daraus erstellte "Auskunftsspiegel" zusammen mit recherchiertem Material in Akten abgelegt wird.

In den restlichen 17 Ermittlungsverfahren, die angebliche Datenschutzverstöße von Auskunfteien, die nicht automatisierte Datenverarbeitung betrieben, zum Gegenstand hatten, wurde indessen die Dateifrage von den Staatsanwaltschaften nicht angesprochen. Als Grund für dieses Verhalten bieten sich zwei Erklärungen an: Zum einen ist möglich, daß die Staatsanwaltschaften "wie selbstverständlich" von der h. M., die Auskunfteien in den Anwendungsbereich des BDSG einbezieht [65], ausgegangen sind. Zum anderen könnte ein verweisungsbedingter Grund vorliegen. Denn wenn der von § 41 BDSG ausgehende implizite Verweis auf § 1 II BDSG und von dort auf die Dateidefinition in § 2 III Nr. 3 BDSG nicht durchgeführt wurde, konnte auch keine Interpretation des Dateibegriffs erwartet werden. Eine abschließende Bewertung dieses Verhaltens war indessen durch eine reine Aktenanalyse nicht möglich. Nach meiner (subjektiven) Einschätzung ist allerdings die zweite Alternative wahrscheinlicher.

Auch in den drei Verfahren, in denen zwar Karteien nichtöffentlicher Stellen vorlagen, diese jedoch nicht im Zusammenhang mit Auskunfteien standen, waren in allen Fällen keine Vermerke oder Andeutungen zur Dateieigenschaft zu finden [66]. Bei einem dieser Verfahren (Fall 13"Betriebsrat") verneinte die Staatsanwaltschaft die Anwendbarkeit des § 41 BDSG aufgrund § 1 II 2 BDSG ("interne Daten"), womit zu vermuten ist, daß der Staatsanwalt sich zumindest gedanklich mit der Dateifrage auseinandergesetzt hatte:

65) Vgl. die Nachweise bei FN 63.

66) Fälle 13 ("Betriebsrat"), 38 ("Karteikastenraub") und 66 ("Versicherungskarteikarten").

Fall 13 ("Betriebsrat"): [67]

Ein Firmeninhaber hatte Karteikarten, die die Fehl- und Krankheitstage von Betriebsräten enthielten, im Betrieb vorgezeigt. Die Staatsanwaltschaft stellte das Verfahren gemäß § 170 II StPO ein: "Die Karten sind für den innerbetrieblichen Geschäftsablauf bestimmt. Aufgrund dessen bedeutet ihr Vorzeigen innerhalb des Betriebes auch keinen Verstoß gegen § 41 BDSG."

b) Karteien von Behörden und sonstigen öffentlichen Stellen

Unter die Rubrik "Karteien der Behörden und sonstigen öffentlichen Stellen" wurden auch die sog. öffentlichen Register [68], wie z. B. Schuldnerverzeichnis, Kfz-Zulassungsstelle oder Einwohnermelderegister, gezählt, wobei indessen nur die Verfahren dazugerechnet wurden, bei denen (noch) die herkömmliche, "manuelle" Registerführung vorlag.

Bejaht man den Dateicharakter von Karteien [69], so liegt in allen hier erfaßten Fällen eine Datei vor. Dies gilt insbesondere auch für die öffentlichen Register, die strukturell eine großformatige Kartei darstellen [70].

Die Behandlung der 18 Ermittlungsverfahren durch die Staatsanwaltschaft war unterschiedlich:

67) Die ausführliche Darstellung des Falls im Anhang.

68) Die Darstellung in der Literatur beschränkt sich weitgehend auf das Problem "allgemein zugängliche Quelle"; vgl. z. B. Simitis in: Simitis/D/M/R § 23 RN 84 und Mallmann in: Simitis/D/M/R § 32 RN 19. Lediglich Schweinoch/Geiger Anm. 2 zu Art. 24 BayDSG bringen expressis verbis zum Ausdruck, daß Melderegister Dateien sind. Das Problem wird sich in Zukunft erübrigen, da dann alle Melderegister "elektronisiert" sind.

69) Vgl. oben die Nachweise bei FN 50 - 52.

70) Wie bei FN 68 ausgeführt, beschäftigt sich die Literatur mit den Registern vorwiegend unter dem Aspekt "allgemein zugängliche Quelle". Man kann daraus schließen, daß sie die Register als vom Anwendungsbereich umfaßt ansieht.

aa) In 12 Verfahren wurde auf die Frage der Dateieigenschaft überhaupt nicht eingegangen; zehnmal erfolgte dabei eine Einstellung gemäß § 170 II StPO mangels Tatverdacht [71], in einem Verfahren wurde nach § 152 I StPO eingestellt [72] und in einem weiteren erfolgte ein Freispruch "aus tatsächlichen Gründen" [73].

Auch hier drängt sich der Verdacht auf, daß die Verweisungskomplexität Ursache für die Nichtbehandlung der Dateifrage ist. Wo oftmals der Anwendungsbereich eines Landesdatenschutzgesetzes einschlägig gewesen wäre, wurde teilweise nur "das Datenschutzgesetz", teilweise das BDSG herangezogen. Wenn aber entweder die Existenz eines Landesdatenschutzgesetzes übersehen wurde, oder aber die Subsidiaritätsregel des § 7 II BDSG überlesen wurde, so spricht dies dafür, daß auch die stillschweigende Verweisung auf Anwendungsbereich und Dateidefinition nicht vollzogen wurde.

bb) In drei Verfahren wurde nicht einmal mehr ein Datenschutzgesetz angeführt, sondern lediglich die Einstellung "mangels strafbarer Handlungen" verfügt.

cc) In den restlichen drei Verfahren wurde von Staatsanwaltschaft oder Gericht die Frage der Dateieigenschaft angesprochen:

In einem Verfahren blieb jedoch offen, ob die Einstellung erfolgte, weil eine Kartei, oder weil interne Daten vorlagen:

71) Hiervon wird vorgestellt Fall 24 ("Mitgliederabwerbung").

72) Fall 50 ("Nötigungsversuch").

73) Fall 40 ("Zentralnamenskartei").

Fall 14 ("Häftlingsadresse"):

Häftling H bekam laufend Werbematerial in die Justizvollzugsanstalt zugesandt. Er erstattete deshalb Anzeige gegen die Anstalt "wegen Verstoßes gegen das Datenschutzgesetz", da nur von ihr die Adressenmitteilung kommen könne. Die Staatsanwaltschaft stellte das Verfahren ein, da sich die Adresse zwar in einer "hausinternen Kartei der Anstalt" befinde, diese aber nicht dem Landesdatenschutzgesetz unterfalle.

Im Fall 15 ("Nachbarsjunge") [74] prüfte zwar die Polizei die Dateifrage, die Staatsanwaltschaft hingegen stellte das Verfahren aus anderen Gründen ein:

Eine bei der Kriminalpolizei beschäftigte Angestellte wollte wissen, ob über den Nachbarsjungen eine Kriminalakte angelegt war. Dazu brachte sie an ihrem Arbeitsplatz nur eine entsprechende Indexkarte zu ziehen und so die Aktennummer feststellen und dann die Akte zur Hand nehmen. Das mit dem Fall befaßte Landeskriminalamt stellte fest, daß das Vorliegen einer Datei notwendig sei. Die Aktenindexkartei sei zwar eine Datei, tatsächlich sei aber die Auskunft aus der Aktensammlung (die keine Datei sei) erteilt worden, was aber wiederum nur über die Indexkartei möglich gewesen sei.

Die Staatsanwaltschaft verneinte eine strafbare Handlung: "Die Strafvorschrift ist nicht anwendbar, weil der Index für die Kriminalakten nicht für Dritte bestimmt ist und in einem nichtautomatisierten Verfahren erstellt wird."

Im letzten, bereits oben angesprochenen Verfahren (Fall 5 "Vorstandsvorsitzender") [75] fanden sich in den staatsanwaltschaftlichen Akten keine Aussagen zum Dateicharakter. Das Gericht hingegen machte Ausführungen und stufte eine Kartei als Datei im Sinne des BDSG ein.

74) Ausführliche Falldarstellung im Anhang.

75) Siehe oben, § 5 A IV, sowie die ausführliche Darstellung im Anhang.

2) LISTEN

Unter einer Liste versteht man eine nur nach einem Kriterium geordnete fortlaufende Sammlung von Daten [76]. Nach vereinzelter Ansicht [77] kann auch sie eine Datei darstellen, da auch sie umgeordnet und - nach anderen Merkmalen geordnet - neu erstellt werden kann. Auf der anderen Seite wird von der überwiegenden Literatur diese Auffassung abgelehnt, da die Umordnung nur durch Erstellen einer neuen Liste möglich sei [78]. Aus Veröffentlichungen sind der Beschluß des VG München [79] und die Verfügung der Staatsanwaltschaft Berlin [80] bekannt:

Nach dem VG München "unterscheidet sich eine Datei von der nur nach einem Merkmal geordnete Liste". Eine tabellarische Auflistung stelle allenfalls eine Liste, jedoch keine Datei dar. Auch die Staatsanwaltschaft Berlin lehnte es ab, den Dateibegriff auf Listen auszudehnen.

Bei der Auswertung konnten in sechs Verfahren Listen als die entscheidenden Speicherorte ermittelt werden:

a) Zwei Verfahren wurden von der Staatsanwaltschaft nach § 170 II StPO mit der Begründung eingestellt, eine Liste sei keine Datei:

76) Vgl. dazu Auernhammer, Kommentar, § 24 RN 16 und Lüke NJW 1983, 1408.

77) Grell, § 4 LDSG BW, RN 40; Louis RN 52.

78) Auernhammer, Kommentar, § 2 RN 24; Dammann in: Simitis/D/M/R § 2 RN 187; Ordemann/Schomerus § 2 Anm. 3.3.1; Leib ÖVD 7 - 8/1978, 23; Lüke NJW 1983, 1408; Schulz BKK 1978, 58; Bull/Zimmermann FuR 1979,121; Bull AfP 1978, 114; Weise DuD 1980, 140; Schweinoch/Geiger Anm. 13 zu Art. 5 BayDSG; Kutzmann Anm. 5.7. zu § 3 LDatG RP; Tubies DuD 1979, 158; wohl auch Bergmann/Möhrle Anm. 10.4 zu § 2.

79) VG München NJW 1981, 475 = DuD 1981, 129.

80) Das Verfahren konnte für die Auswertung nicht erlangt werden, es ist jedoch im Anhang abgedruckt, sowie in DuD 1982, 56 = DANA 2/3/1982, 11 f. dargestellt.

Fall 16 ("Drittschuldnerliste"):

Ein Drittschuldner erhielt einen Pfändungs- und Überweisungsbeschluß, dem als Anlage eine Liste mit Name, Anschrift und Schuldgrund von 21 weiteren Drittschuldnern beigefügt war.

Fall 17 ("Aktienhandel"):

Auf losen, mit Schreibmaschine beschriebenen Blättern waren Aktionäre einer bestimmten Aktiengesellschaft mit Name, Anschrift, Aktienzahl und gewünschtem (Verkaufs-)Kurs notiert. Der Beschuldigte, ein Händler, ließ sich dahingehend ein, er habe sie auf der Hauptversammlung von einem Unbekannten erhalten.

b) Zwar erfolgte auch bei den restlichen vier Verfahren eine Einstellung nach § 170 II StPO, doch wurde dabei nicht die fehlende Dateieigenschaft von Listen als Grund angegeben. Vielmehr ermittelte die Staatsanwaltschaft in allen Verfahren wegen Datenschutzverstößen. Es bieten sich zwei Erklärungen für dieses Vorgehen an:

Zum einen könnten die Staatsanwälte (wie auch die jeweiligen Verteidiger der Beschuldigten) Listen stillschweigend als Dateien und damit vom Anwendungsbereich der Datenschutzgesetze umfaßt angesehen haben. Es läge ein "bloßer" Subsumtionsfehler vor.

Ein anderer Grund für diese Vorgehensweise könnte darin liegen, daß die Staatsanwälte beim bloßen Wortlaut der Datenschutzgesetze stehengeblieben sind und den Weiterverweis auf Anwendungsbereich und von dort auf die Dateidefinition nicht vollzogen haben. Sollte dies der Grund gewesen sein, wäre die Einbeziehung der Listen als verweisungsspezifischer Fehler zu qualifizieren.

Aus dieser Gruppe seien zwei Verfahren vorgestellt:

Fall 18 ("Werbeliste"):

Ein Versicherungsvertreter war im Besitz einer Liste mit einzustellenden Nachwuchskräften einer Stadtverwaltung, die er wahrscheinlich von einem dortigen Mitarbeiter erhalten hatte. Er besuchte die aufgelisteten Personen und versuchte sie zum Abschluß einer Versicherung bei seiner Gesellschaft zu bewegen.

Fall 19 ("Roulettspieler"): [81]

Verschiedene Spielbanken sandten sich gegenseitig Schreiben, auf denen angebliche "Mitglieder einer internationalen Berufsspielerorganisation" aufgelistet waren. Nachdem der dort aufgeführte Roulettspieler R mehrfach aus Spielbanken verwiesen worden war, stellte er Strafantrag.

Der von der h. M. vorgetragenen Ansicht, wonach Listen keine Dateien darstellen [82], ist zuzustimmen. Die Datenschutzgesetze wurden geschaffen, um die sich aus der automatischen Datenverarbeitung ergebenden (neuartigen) Gefahren zu beherrschen, nicht aber, um herkömmliche Informationsinstrumente der "Papiertechnologie", wie (isoliert verwandte) Listen oder Akten, einzubeziehen. Es kann Grell auch nicht gefolgt werden, wenn er ausführt, die Verfügbarkeit sei bei Listen nicht geringer als bei einer Kartei [83]. Eine Liste muß für jede Umordnung (und damit auch für die Wiederherstellung des ursprünglichen Zustandes) zerstört werden, während bei einer Kartei auch vielfache Umordnungen nach verschiedenen wechselnden Kriterien möglich sind. Die eben vorgestellten Verfahren können als zusätzliches, "empirisches" Argument gegen eine Einbeziehung der Listen in den Dateibegriff herangezogen werden: Sie repräsentieren Fälle "klassischen" Datenmißbrauchs, nicht aber computerspezifische Vorgehensweisen, womit keine Notwendigkeit besteht, sie in den Anwendungsbereich der Datenschutzgesetze einzubeziehen.

81) Ausführliche Falldarstellung im Anhang.

82) Vgl. FN 78 - 80.

83) Grell, § 4 LDSG BW, RN 40.

3) MIKROFICHES und MIKROFILME [84]

Bei der Beurteilung der Dateieigenschaft von Mikrofiche und Mikrofilm ist, entsprechend der unterschiedlichen physischen Beschaffenheit, eine differenzierte Betrachtung nötig.

a) Einem Mikrofilm wird von der ganz überwiegenden Literaturmeinung keine Dateieigenschaft zugesprochen [85]. Soweit ersichtlich, ist nur Grell anderer Ansicht [86], da er Mikrofilme den Listen, denen er Dateiqualität beimißt, gleichstellt. Insofern ist hier auf das eben zu den Listen gesagte zu verweisen und diese Ansicht abzulehnen [87].

Die Staatsanwaltschaft war nur in einem der hier vorliegenden Verfahren (Fall 20 "Bibliotheksbenutzerausweis") mit Mikrofilmen beschäftigt, ließ die Frage der Dateieigenschaft jedoch offen:

Fall 20 ("Bibliotheksbenutzerausweis"): [88]

Die Benutzerausweise einer Bibliothek waren kopiert und fortlaufend auf Mikrofilm gespeichert. Als durch eine Panne Daten weitergegeben worden waren, erklärte der beschuldigte Direktor, seine Aufsichtsbehörde und er seien der Meinung, Mikrofilme seien keine Dateien. Die Staatsanwaltschaft stellte das Verfahren mit der Begründung ein, es habe hier nur fahrlässiges und damit strafloses Handeln vorgelegen. Die Frage der Dateieigenschaft sei daher nicht zu entscheiden.

84) Vgl. hierzu auch die von der Bundesregierung beschlossenen Richtlinien für die Mikroverfilmung, abgedruckt in BKK 1978, 374 - 376.

85) Auernhammer, Kommentar, § 2 RN 24; Ordemann/Schomerus § 2 Anm. 3.3.1; Dammann in: Simitis/D/M/R § 2 RN 1983; Hund DSWR 1977, 46; Schulz BKK 1978, 58;Hergenhahn DuD 1977, 26; Weise DuD 1980, 142; Kutzmann Anm. 5.7. zu § 3 LDatG RP.

86) Grell, § 4 LDSG BW, RN 40.

87) Siehe oben, § 5 A V 2).

88) Ausführliche Falldarstellung im Anhang.

b) Die Beurteilung, ob ein oder mehrere Mikrofiches eine Datei darstellen, hängt von der konkreten Fallkonstellation ab [89].

Unproblematisch sind die Fälle, in denen die Mikrofiches im sog. COM-Verfahren [90] hergestellt werden [91]. Das (unberechtigte) Kopieren auf Mikrofiches (oder auf Mikrofilm) mit Hilfe der Datenverarbeitungsanlage ist dann als (unbefugtes) Abrufen zu qualifizieren [92].

Gleiches gilt für die Fälle, in denen die Mikrofiches durch Vorschalten eines automatischen Suchsystemes umgeordnet und ausgewertet werden können [93].

Solange mehrere Mikrofiches vorhanden sind, die ähnlich wie eine Kartei umgeordnet und ausgewertet werden können, liegt eine Datei vor [94]. Ein einzelner Mikrofiche muß dann aber die Funktion einer Karteikarte haben [95].

Liegt dagegen nur ein einzelner Mikrofiche vor oder aber sind die mehreren Mikrofiches nicht karteimäßig aufgebaut, so besteht eine strukturelle Gleichheit mit den Listen und es ist keine Datei gegeben [96]. Denn dann ist innerhalb eines einzelnen Mikrofiches eine physische Umsortierung nicht möglich, es sei denn, man zerschneidet ihn.

89) Auernhammer, Kommentar, § 2 RN 24; Dammann in: Simitis/D/M/R § 2 RN 193; Heinemann DOK 1978, 413;Schweinoch/Geiger Anm. 16 zu Art. 5 BayDSG.

90) Computer-Output-Microfilm; vgl. dazu Schott DSWR 1983, 21 ff.

91) Vgl. nur Dammann in: Simitis/D/M/R § 2 RN 193.

92) Als Beispiel ist hier auf den in § 3, B, der Arbeit vorgestellten Fall 1 ("Universitätsoperator") zu verweisen.

93) Schweinoch/Geiger Anm. 16 zu Art. 5 BayDSG.

94) So auch Kutzmann Anm. 5.7. zu § 3 LDatG RP und wohl auch Ordemann/Schomerus § 2 Anm. 3.3.1; Hergenhahn DuD 1977, 26.

95) Kutzmann, Anm. 5.7. zu § 3 LDatG RP.

96) Siehe oben, § 5 A V 2).

Bei vier der hier vorliegenden fünf Verfahren waren Mikrofiches listenartig aufgebaut [97]. Die nur nach dem Kriterium "Namen" geordneten Mikrofiches stellen nichts anderes dar, als verkleinerte Listen.

Von den Staatsanwaltschaften wurde jedoch die Frage der Dateieigenschaft nur in einem der vier Verfahren angeschnitten:

Fall 21 ("Mikrofichesfund"): [98]

Beim Kauf gebrauchter Schreibtische einer Bank fanden sich in den Schubladen auf über einem Dutzend Mikrofichkarten Kundenadressen mit Kreditangaben. Die Beschuldigten versuchten diese für Kreditgeschäfte zu verwerten. Die Staatsanwaltschaft war der Meinung, "daß jede einzelne Mikrofichkarte bereits als Datei im Sinne des § 2 BDSG zu behandeln sei". Weder das erstinstanzliche Gericht, noch das Berufungsgericht gingen auf die Frage der Dateieigenschaft ein, sondern veruteilten die Angeklagten wegen Unterschlagung und Hehlerei.

In den übrigen drei Verfahren kann indessen ein Scheitern an der Verweisungstechnik nicht ausgeschlossen werden. Für die Beschuldigten entstanden in den Verfahren insofern keine negativen Auswirkungen, als die Verstöße gegen die Datenschutzgesetze letztendlich aus anderen Gründen verneint wurden:

Fall 22 ("Spenderlisten"):

Der Beschuldigte stahl Mikrofiches, auf denen Spender einer gemeinnützigen Organisation listenmäßig aufgeführt waren. Die Frage, ob eine Datei vorliegt, wurde nicht angesprochen. Ein Verstoß gegen § 41 BDSG wurde mit folgender Begründung abgelehnt: "Aus den Einlassungen des Beschuldigten ergibt sich, daß sich die sog. Fiche nicht in Behältnissen zur Tatzeit befanden."

97) Listenartiger Aufbau bei den Fällen 22 ("Spenderlisten"), 23 ("Kreditangebote"), 21 ("Mikrofichesfund") und 24 ("Mitgliederabwerbung"). Das fünfte Verfahren war Fall 25 ("Mikroficheeinsicht").

98) Ausführliche Falldarstellung im Anhang.

Fall 23 ("Kreditangebote"): [99]

Kunden einer Bank erhielten plötzlich Kreditangebote von einer Kredit-GmbH. Die Kundenadressen wurden u. a. auf Mikrofiches gespeichert. Nachdem umfangreiche Ermittlungen erfolglos geblieben waren, wurde das Verfahren eingestellt. Die Dateifrage wurde nicht angeschnitten.

Fall 24 ("Mitgliederabwerbung"): [100]

Die Mitglieder einer Krankenkasse erhielten von einem anderen Unternehmen Angebote. Die Mitgliederadressen waren in EDV-Anlagen, Karteien, auf Mikrofiches und Computerausdrucken gespeichert. Die Staatsanwaltschaft ging auf die Dateienfrage nicht ein, sondern stellte das Verfahren mangels Strafantrag eines Berechtigten ein.

Beim fünften Verfahren war aus den Akten nicht zu entnehmen, ob ein listenmäßig aufgebauter Mikrofiche vorlag. Der Beschuldigte wurde dennoch wegen Verstoßes gegen das BDSG verurteilt:

Fall 25 ("Mikroficheeinsicht"): [101]

Der Beschuldigte war ins Arbeitsamt eingedrungen und hatte einen Mikrofiche eingesehen, auf dem seine Leistungsdaten abgelichtet waren. Der von der Staatsanwaltschaft beantragte Strafbefehl wegen Hausfriedensbruch und Verstoß gegen das BDSG wurde mit der Begründung erlassen, der Beschuldigte habe Daten aus seinen Leistungsakten über ein Datensichtgerät eingesehen.

Zur Frage des Dateicharakters wären hier nähere Ermittlungen nötig gewesen. Es hätte geklärt werden müssen, ob der Mikrofiche listenmäßig oder nicht aufgebaut war. Da indessen die Staatsanwaltschaft keinerlei Untersuchungen in dieser Hinsicht unternommen hatte, ist ein Überlesen des Verweises auf den Anwendungsbereich und von dort auf die Dateidefinition zu vermuten.

99) Ausführliche Falldarstellung im Anhang.

100) Ausführliche Falldarstellung im Anhang.

101) Ausführliche Falldarstellung im Anhang.

4) COMPUTERAUSDRUCKE

Bei der Beurteilung von Computerausdrucken ist eine differenzierte Betrachtung nötig:

Auf der einen Seite stehen die Verfahren, in denen der Ausdruck auf eine Manipulation an der EDV-Anlage zurückzuführen ist. Auf der anderen Seite die Fälle, in denen lediglich befugterweise hergestellte Abdrucke entwendet bzw. mißbraucht werden. Nur um diese handelt es sich bei den hier erfaßten acht Fällen [102].

Die Unterscheidung ist deshalb nötig, da sich nur bei der ersten Alternative die spezifischen Gefahren der Datenverarbeitung realisieren. Die Handlungsweise der zweiten Alternative ist auch bisher schon gegeben gewesen. Wenn aber ein Mitarbeiter Unterlagen entwendet, so darf es keinen Unterschied machen, ob er eine Akte oder einen Computerausdruck mitnimmt. Tatobjekt ist jedesmal "das Bündel Papier". Es ist Aufgabe des Betreibers der DV-Anlage, geeignete Sicherungsmaßnahmen zu ergreifen, um unbefugtes Entwenden von Ausdrucken zu erschweren. Datenschutzspezifisch sind nur die Fälle, in denen durch eine Einwirkung auf die EDV-Anlage Informationen erhalten, weitergegeben oder zerstört werden, d. h., wenn Tatobjekt "der Computer" ist.

Damit ist bei Verfahren, in denen die Daten aus einem Ausdruck weitergegeben werden, zu klären, ob der Ausdruck nur mitgenommen wurde (dann § 242 bzw. § 246 StGB) oder aber, ob er aufgrund einer (mittelbaren oder unmittelbaren) Handlung des Beschuldigten zustande kam (dann Verstoß gegen die Strafbestimmungen, namentlich in der Form des Abrufens, der Datenschutzgesetze).

102) Siehe oben, Tabelle 5.5 "Graubereich", § 5 A V.

Entscheidend sind also die tatsächlichen Verhältnisse, d. h. aus welcher Quelle die Daten stammen.

Bedauerlicherweise wurde diese Unterscheidung im Fall 26 ("Zeitungsabonnenten") nicht getroffen. Hier wurde der beschuldigte Programmierer, der einen Kontrollausdruck statt ihn zu vernichten, mitgenommen und dann zu verkaufen versucht hatte, wegen "Übermittlung nach dem Bundesdatenschutzgesetz in Tateinheit mit Diebstahl einer geringwertigen Sache" zu 4 Monaten Freiheitsentzug verurteilt [103].

Bei einer Entwendung von Computerausdrucken muß also entscheidend sein, wie der Täter die Ausdrucke erlangt hat. Dies gilt genauso für den strukturell gleich gelagerten Fall, daß die gleichen Daten in einer Datei und in einer Akte vorhanden sind. Auch hier muß geklärt werden, woraus der Beschuldigte übermittelt hat.

Demgegenüber wird aber von Ordemann/Schomerus folgende Meinung vertreten [104]:
"Werden die Daten tatsächlich aus einer Akte übermittelt, kann eine Übermittlung im datenschutzrechtlichen Sinne vorliegen, wenn dieselben Daten auch in einer Datei gespeichert sind. Mit dem Schutzzweck des Gesetzes wäre es unvereinbar, wenn auf die tatsächlich genutzte Quelle abgestellt würde."

Diese Ansicht widerspricht jedoch dem strafrechtlichen Analogieverbot. Wenn man die Weitergabe von Daten aus Akten an sich (d. h. solange sie "alleine" sind) nicht als Übermittlung im Sinne der Datenschutzgesetze ansieht (wie dies auch Ordemann/

103) Fall 26 ("Zeitungsabonnenten") wird ausführlich im Anhang geschildert.
104) Ordemann/Schomerus § 2 Anm. 2.2.

doch nicht
Schomerus tun), so kann plötzlich eine Übermittlung vorliegen, nur weil (zufällig) dieselben Daten gleichzeitig auch in einer Datei gespeichert sind. Es ist verbotene Analogie, die Fälle der Übermittlung aus einer Datei mit denen der Übermittlung aus Akten (bei gleichzeitigem Vorliegen einer Datei) pauschal gleichzusetzen, ohne auf die tatsächlich genutzte Quelle abzustellen. Auch das Argument, es sei oft sehr schwierig, die wirklich inanspruchgenommene Quelle festzustellen, vermag daran nichts zu ändern. Für eine strafrechtliche Betrachtung ist die Feststellung der tatsächlichen Verhältnisse unentbehrlich. Alles andere würde auf eine Entscheidung "in dubio contra reum" hinauslaufen.

In einem entsprechenden gelagerten Verfahren (Fall 27 "Multifunktionär") hat dann auch die Staatsanwaltschaft zurecht auf die tatsächlich genutzte Quelle abgestellt [105]. Allerdings wurde sie auf das Problem vom Beschuldigten (einem Juristen) aufmerksam gemacht. Dieser gab zwar zu, die Daten aus Akten entnommen zu haben, bestritt jedoch die Anwendbarkeit der Datenschutzgesetze:

Fall 27 ("Multifunktionär"): [106]

Der Kanzler einer Universität versandte an die Mitglieder der Universitätsgremien ein Schreiben, in dem er Daten eines Studenten preisgab. Diese Daten waren sowohl in der EDV-Anlage der Universität, als auch in Akten gespeichert. Die Staatsanwaltschaft stellte das Verfahren ein: Der Beschuldigte habe die Daten aus studentischen Akten entnommen; das Landesdatenschutzgesetz setzte aber eine Datei als Quelle voraus.

105) Vgl. dazu auch die Fälle 23 ("Kreditangebote"), 24 ("Mitgliederabwerbung") und 5 ("Vorstandsvorsitzender"), in denen die Daten ebenfalls nicht nur in EDV-Anlagen, sondern auch in Akten bzw. ("listenartigen") Mikrofiches gespeichert waren.

106) Ausführliche Falldarstellung im Anhang.

B) Ausgrenzungen vom Anwendungsbereich

Vom Schutz des Gesetzes sind die sog. "internen Daten" und die unter das sog. "Medienprivileg" fallenden Daten ausgenommen [107].

I) INTERNE DATEN

Sogenannte "interne Daten" liegen vor, wenn kumulativ zwei in § 1 II 2 BDSG statuierte Voraussetzungen erfüllt sind [108]:

- Erstens dürfen die Daten nicht zur Übermittlung an Dritte [109] bestimmt sein und

- zweitens müssen sie in nicht automatisierten Verfahren verarbeitet werden.

Somit fallen z. B. private - in Dateiform geführte - Telefonverzeichnisse oder Handkarteien darunter [110].

Nach dem eindeutigen Wortlaut der Datenschutzgesetze gilt bei internen Daten nur die (jeweilige) Vorschrift für die Datensicherung [111], nicht aber die Strafbestimmung. Aus strafrechtlichen Gesichtspunkten ist jedoch die aus dieser Einteilung in interne und sonstige Daten folgende Straflosigkeit der Täter, die sich "nur" interne Daten verschaffen oder weitergeben,

107) Beim BDSG gilt jeweils nur § 6 BDSG ("Technische und organisatorische Maßnahmen zur Datensicherung"). Entsprechendes gilt für die Landesdatenschutzgesetze.

108) Diese Sonderregelung war von Anfang an umstritten. Vgl. Simitis in: Simitis/D/M/R § 1 RN 30 mwN. Auch bei den Landesdatenschutzgesetzen sind die "internen Daten" aus dem Anwendungsbereich ausgenommen: § 1 II 2 LDSG BW; Art. 1 II 2 BayDSG; § 3 III BlnDSG; § 1 II 3 BrDSG; § 1 II 2 HmbDSG; § 1 II 2 LDSG NW; § 2 II LDatG RP; § 1 II 2 SDSG; § 3 IV LDSG SH.

109) Für die Bestimmung des "Dritten" ist die Legaldefinition in § 2 II Nr. 2 BDSG heranzuziehen. Entsprechendes gilt bei den Landesdatenschutzgesetzen.

110) Ordemann/Schomerus § 1 Anm. 4.

111) So wird z. B. beim BDSG auf dessen § 6 verwiesen. Wie indessen Simitis in: Simitis/D/M/R § 1 RN 31 ausführt, ist die Verweisung auf § 6 BDSG in dieser globalen Form verfehlt. Die Anwendbarkeit von § 6 II BDSG scheidet von vornherein aus.

wenig überzeugend [112]. Zum einen kann es sich rein zufällig um interne Daten handeln, zum anderen kann gerade ihnen ein besonderer Vertrauensbruch zugrundeliegen. Weiter ist möglich,daß gerade interne Daten besonders gesichert sind und damit eine erhöhte kriminelle Energie nötig ist, um diese besonderen Sicherungsvorkehrungen auszuschalten. Zwar mag es anderen datenschutzrechtlichen oder sonstigen Erwägungen folgend sinnvoll sein, für interne Daten nur Datensicherungsmaßnahmen vorzuschreiben, vom Standpunkt des Strafrechts aber ist dies nicht der Fall.

De lege ferenda sollte deshalb von einer Herausnahme der internen Daten aus dem Schutzbereich der Strafbestimmungen abgesehen werden.

Da indessen bei der Untersuchung von der tatsächlichen Rechtslage auszugehen war, mußte geprüft werden, inwieweit die verweisungsdeterminierte Herausnahme der internen Daten aus dem Schutzbereich der Strafbestimmungen von den Strafverfolgungsbehörden gesehen wurde.

Erforderlich war zunächst die Aussonderung des relevanten Fallmaterials.

1) Verarbeitung in nicht automatisierten Verfahren

Erste Bedingung für "interne Daten" ist die Verarbeitung dieser in nicht automatisierten Verfahren. Da in EDV-Anlagen personenbezogene Daten in automatisierten Verfahren bearbeitet werden, stellte sich die Frage nicht bei den unter der Rubrik "EDV-Anlagen" erfaßten 61 Verfahren [113]. Auch die Fälle, bei denen

112) Nach Simitis NJW 1981, 1699 liegt in § 1 II BDSG die größte Gefahr für den Datenschutz. Kritisch auch Meister, Datenschutz, S. 28 und Bull, Ziele, S. 26; sowie die GMD-Studie S. 50.

113) Siehe oben, § 5 A II, Tab. 5.1 "Speicherorte ("Quelle")".

keine Datei vorlag sind auszuscheiden, da sie nicht unter den Anwendungsbereich des Gesetzes fallen und somit auch nicht von der Unterausnahme des § 1 II 2 BDSG erfaßt werden können [114]. Damit waren die 40 Nicht-Datei-Fälle [115] ebenso außer Betracht zu lassen, wie die in der Rubrik "Graubereich" aufgeführten "Listenfälle" [116], die zwanzigmal vorkamen.

Es blieben somit 39 Verfahren der Rubrik "Graubereich", bei denen eine "Verarbeitung im nicht automatisierten Verfahren" vorlag.

2) Nicht zur Übermittlung an Dritte bestimmt

Die zweite Voraussetzung für interne Daten ist, daß die Daten "nicht zur Übermittlung an Dritte bestimmt" sind. Die Interpretation dieser Formulierung ist jedoch umstritten. Nach einer Mindermeinung kann allein der Dateninhaber entscheiden, welche Daten nicht zur Übermittlung an Dritte bestimmt sind, d. h., er kann durch seinen Willen Daten zu "internen" machen (streng subjektive Sicht) [117]. Nach der herrschenden Meinung ist es allein objektiv zu beurteilen, ob die Daten zur Übermittlung bestimmt sind [118]. Eine dritte Gruppe fordert eine Übereinstimmung der subjektiven Zweckbestimmung mit den objektiven Gegebenheiten, bzw., daß Daten erst durch eine (subjektive) Entscheidung zu Internen werden und diese Entscheidung aber einen objektiven Niederschlag gefunden haben müsse [119].

114) Ordemann/Schomerus § 1 Anm. 4; BT-Drs. 7/1027 S. 18.

115) Siehe oben, § 5 A II, Tab. 5.1 "Speicherorte ("Quelle")".

116) Hierunter fallen die Gruppen "Mikrofilm und Mikrofiche", "Listen", sowie "Computerausdrucke".

117) Hörle/Wronka § 1 RN 13 ff; Schwappach § 1 Anm. 4 f.

118) Lilie S. 162; Wohlgemuth S. 17; Simitis NJW 1977, 733; ders. in: Simitis/D/M/R § 1 RN 35; wohl auch Louis RN 57.

119) Auernhammer, Kommentar, § 1 RN 11; Ruckriegel, Kommentar, Erl. 9 zu § 1 LDSG NW; Ordemann/Schomerus § 1 Anm. 4; Gallwas in: Gallwas/S/S § 1 RN 37.

Am besten mit dem Sinn und Zweck des Datenschutzes läßt sich die Ansicht vereinbaren, die sich für eine rein objektive Betrachtung ausspricht, denn ansonsten könnte ein Datenbesitzer nach Belieben den Umfang der für ihn geltenden Regelungen bestimmen. Der Anwendungsbereich eines Gesetzes kann aber nicht der Verfügbarkeit eines Dritten unterworfen werden. Es kann vom Gesetzgeber nicht gewollt gewesen sein, daß die Bekämpfung der von ihm erkannten Mißbrauchsgefahren durch eine autonome Entscheidung des Datenverarbeiters unterlaufen werden kann. Diese Überlegungen gelten auch für die dritte Ansicht (subjektiv-objektive Betrachtung), da auch hier über die subjektive Komponente die Gefahr bestehen bleibt, die Bestimmungen des BDSG zu unterlaufen, indem etwa objektive Gegebenheiten vorgeschoben oder konstruiert werden [120].

Ohne Auswirkungen bleibt der Streit bei personenbezogenen Daten, die aufgrund gesetzlicher oder rechtsgeschäftlicher Verpflichtungen an Dritte übermittelt werden müssen. Hier ist man sich einig, daß sie von § 1 II 2 BDSG ausgenommen sind [121]. Selbst Schwappach, der als Vertreter der Gegenmeinung zitiert wird, stimmt der obigen Auffassung für die Fälle zu, in denen der Datenverarbeiter "zumindest auch aus eigenem Interesse" die Daten zur Verfügung stellt und führt als Beispiel die Übermittlung von Arbeitnehmerdaten an die Sozialversicherung auf [122].

Von den 39 Fällen, in denen eine Verarbeitung in nicht-automatisierten Verfahren stattfand, war 23 mal von einer objektiven wie subjektiven Bestimmung zur Übermittlung auszugehen.

120) Meister ZRP 1979, 132; Simitis NJW 1977, 733.

121) Ordemann/Schomerus § 1 Anm. 4.; Simitis in: Simitis/D/M/R § 1 RN 36; Auernhammer, Kommentar, § 1 RN 11; Lilie S. 161; Louis RN 57; Schwan in: Burhenne/Perband § 1 RN 90.

122) Schwappach Erl. 5 zu § 1.

Das waren z. B. die Fälle, in denen Daten von Auskunfteien, Schuldnerverzeichnissen oder Einwohnermeldeämtern und ähnlichen weitergegeben wurden. In diesen 23 Fällen konnten somit keine internen Daten vorliegen.

Übrig blieben so 13 Verfahren, in denen möglicherweise interne Daten vorlagen. Sie wurden im Hinblick darauf untersucht, ob die Staatsanwaltschaften diese Möglichkeit sahen und wie sie die Fälle lösten. Dabei wurde festgestellt, daß die Herausnahme der internen Daten aus dem Schutzbereich der Datenschutzgesetze von der Staatsanwaltschaft oder Polizei nur in drei der dreizehn Verfahren angesprochen wurde[123]. Wenn somit auf der anderen Seite in zehn Fällen das Problem der internen Daten überhaupt nicht erkannt wurde, so spricht dies für den Nichtvollzug der Verweisung auf § 1 II BDSG. Die Strafverfolgungsbehörden hatten also auch hier mit verweisungsspezifischen Schwierigkeiten zu kämpfen.

123) Es handelt sich um die bereits vorgestellten Fälle 15 ("Nachbarsjunge"), 13 ("Betriebsrat"), sowie 14 ("Häftlingsadresse").

II) MEDIENPRIVILEG

In § 1 III BDSG (und entsprechendes gilt für die Landesdatenschutzgesetze) [124] ist das sog. "Medienprivileg" [125] statuiert:

§ 1 III BDSG

"Dieses Gesetz schützt personenbezogende Daten nicht, die durch Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Films ausschließlich zu eigenen publizistischen Zwecken verarbeitet werden; § 6 Abs. 1 bleibt unberührt."

Bei der allgemeinen Beurteilung des Medienprivilegs gehen die Meinungen auseinander, wobei sogar zum Teil die Verfassungswidrigkeit des Medienprivilegs behauptet wird [126]. Der überwiegende Teil der Literatur [127] fordert den Gesetzgeber zum Tätigwerden auf, da das Medienprivileg eine "offene Flanke" für den Datenschutz bedeute [128] und eine "Datenschutz-Immunität" darstelle [129]. Doch dieser Appell ist auch das einzige, worin man sich einig ist, denn wie eine Änderung aussehen soll, ist umstritten. Es werden vier Lösungen angeboten:

124) Vgl. § 1 III LDSG BW; Art. 21 BayDSG; §§ 3 III, 27 BlnDSG; §§ 1 V, 29 BrDSG; §§ 3 III, 31 HDSG; § 2 IV HmbDSG; § 1 III NDSG; §§ 1 III, 32 LDSG NW; § 24 LDatG RP; § 23 SDSG; vgl. auch § 3 III LDSG SH.

125) Demgegenüber möchte Hendriks FuR 8/1979 S. 407, daß vom "publizistischen Vorbehalt" gesprochen wird.

126) Schwan in: Burhenne/Perband § 1 RN 95, 97.

127) Helmig S. 129; Bull FuR 8/1979 S. 400; ders. DuD 1982, 149; ders. AfP 1978, 112; Louis RN 61; Heussner, FS Wannagat S. 187; Bull/Zimmermann FuR 3/1979 S. 118; Ordemann/Schomerus § 1 Anm. 5; Simitis DuD 1982, 241; ders. FS Löffler S. 322; Hempelmann FuR 8/1979 S. 412; O. Mallmann NJW 1981, 138; Erklärung des DGB, abgedruckt in DANA 6/1982 S. 19; Wronka FuR 3/1979 S. 123. Ebenso der Bericht des Bayer. Staatsministeriums des Innern (aufgrund Beschluß des Bayer. Landtages vom 30.1.1980 - Drs. 9/3863) vom 12. Juni 1981, Geschäftszeichen I A 7-476-1/3 (80) S. 19, kritisch auch Kröger DÖV 1977, 302. Gegen eine Änderung: Hendriks FuR 8/1979 S. 409.

128) Bull FuR 8/1979 S. 402.

129) Bull/Zimmermann FuR 3/1979 S. 121.

1) Das Medienprivileg wird ersatzlos gestrichen, da es eine nicht gerechtfertigte und verfassungswidrige Ausnahmeregelung darstellt. Auch die Presse müsse dem BDSG unterfallen 130.

2) § 1 III BDSG wird zwar gestrichen, da auch die Presse grundsätzlich unter das BDSG fallen müsse, jedoch sollten im Gesetz umfangreiche und umfassende Sondervorschriften für die Presse geschaffen werden 131. Einen kleinen Schritt in diese Richtung enthielt der Referentenentwurf zur Änderung des BDSG 132, wobei es allerdings beim grundsätzlichen Ausschluß der Presse vom Anwendungsbereich des BDSG verbleiben sollte. Neu war nur die Verpflichtung zur Sicherung einer Gegendarstellung mit den sie auslösenden Informationen, sowie ein beschränktes Auskunftsrecht. Daneben sollten die Rundfunkanstalten des Bundesrechts einen Datenschutzbeauftragten bestellen.

3) Das Medienprivileg des BDSG bleibt bestehen, es soll jedoch eine bereichsspezifische Regelung 133 (was wohl einem eigenen Pressedatenschutzgesetz gleichkommt) geschaffen werden; dazu sei der Gesetzgeber verpflichtet 134.

4) Das Medienprivileg wird erweitert, da es nicht weitgehend genug ist und deshalb "bei einer restriktiven Auslegung die Pressedatenbanken jederzeit lahmgelegt werden können" 135.

Es ginge zu weit und ist auch nicht Ziel der Arbeit, speziell zu diesem Komplex umfassend Stellung zu nehmen [136]. Es soll jedoch auf folgendes hingewiesen werden:

130) So die Erklärung des DGB, abgedruckt in DANA 6/1982 S. 19.

131) Helmig S. 129, der auf S. 130 ff. Vorschläge für solche Vorschriften macht.

132) § 1 a des Referentenentwurfs vom 23.6.1983, abgedruckt in DANA 5/1983 S. 5 - 10. Er wurde inzwischen, nach Erlaß des Volkszählungsurteils des BVerfG (E 65, 1 ff.), zurückgezogen und soll überarbeitet werden; dazu Herb, computer magazin, Heft 6/1984 S. 6.

133) Bull FuR 8/1979 S. 400 ders. AfP 1978, 112; Louis RN 61; Heussner, FS Wannagat S. 187; Bull/Zimmermann FuR 3/1979, 118; Ordemann/Schomerus § 1 Anm. 5; Woertge S. 150.

134) Simitis DuD 1982, 241; wohl auch Garstka JZ 1978, 511 ; Simitis in: Simitis D/M/R § 1 RN 50; Simitis FS Löffler S. 322.

135) Hempelmann FuR 8/1979 S. 412.

136) Eine sehr ausführliche Kommentierung findet sich z. B. bei Hörle/Wronka § 1 RN 20 - 81 (= S. 21 - 49).

Geht man davon aus, daß das BDSG die besonderen Gefahren der Datenverarbeitung in den Griff bekommen will, so ist wenig einsichtig, weshalb die Mißbrauchsgefahr bei EDV-Anlagen bei Behörden oder privaten Unternehmen höher sein soll als bei Zeitung, Film oder Funk. Beidesmal handelt es sich um Datenverarbeitungsanlagen, die personenbezogene Daten speichern, ja es kann sogar vorkommen, daß Hard- und Software identisch sind, es sich also um das gleiche Hilfsmittel, das gleiche Werkzeug handelt. Ob Mißbrauch getrieben wird, hängt allein ab von den Benutzern, den Zugriffsberechtigten [137], denn das "Werkzeug Computer" ist in dieser Beziehung völlig neutral. Wenn (der Journalist) Hempelmann in seiner Polemik dem BDSG unterstellt, es "scheide die Menschheit in zwei Informationsklassen, nämlich a) Journalisten und b) Sonstige" [138], so fällt dieser Vorwurf auf ihn selbst zurück: Wenn Journalisten keine "besseren oder schlechteren Menschen" sind, ist kein Grund ersichtlich, ihnen (und ja nur ihnen) sorgfältigeren, d. h. "mißbrauchsloseren" Umgang mit dem Werkzeug Computer zu unterstellen, mithin sie durch § 1 III BDSG zu privilegieren. Der bloße Hinweis auf Art. 5 GG (Pressefreiheit) verkennt, daß sich ja auch der Betroffene auf grundgesetzliche Positionen berufen kann. Die Datenschutzgesetze wurden zum Schutz der Privatsphäre und damit der Würde des Einzelnen geschaffen. Das BVerfG betont im Volkszählungs-Urteil ausdrücklich das "informationelle Selbstbestimmungsrecht" des Einzelnen über seine Daten als Ausfluß des allgemeinen Persönlichkeitsrechts des Art. 2 I iVm Art. 1 I GG [139]. Die Meinungsfreiheit ist - wie Simitis zurecht darlegt - "kein Freibrief vom Datenschutz" [140] und "die Pressefreiheit verlangt kein datenschutzrechtliches Vakuum" [141].

137) So auch zurecht Helmig S. 113 und S. 129.

138) Hempelmann S. 412.

139) BVerfGE 65, 1 ff. = NJW 1984, 419 ff.

140) Simitis DuD 1982, 248.

141) O. Mallmann NJW 1981, 138.

Nach dem eindeutigen Wortlaut indessen führt die de lege lata statuierte Herausnahme der von den Medien verarbeiteten Daten aus dem Anwendungsbereich der Datenschutzgesetze dazu, daß diese Daten auch keinen strafrechtlichen Schutz genießen. Es ist strukturell die gleiche Konstruktion, wie bei den internen Daten [142]. Da die personenbezogenen Daten, die "durch ... Unternehmen ... der Presse ... verarbeitet werden", nicht "von diesem Gesetz geschützt" sind [143], unterfallen sie auch nicht dem Schutz der Strafbestimmungen. Es war deshalb zu untersuchen, inwieweit die Staatsanwaltschaften die verweisungsdeterminierte Herausnahme der vom Medienprivileg erfaßten Daten aus dem Schutzbereich der Strafnormen bewältigt haben.

Die Auswertung ergab, daß von den 159 Verfahren in nur drei Fällen [144], die sogleich vorgestellt werden, § 1 III BDSG relevant wurde [145]. Hinzu kommt noch der bereits oben vorgestellte Fall der Staatsanwaltschaft Berlin [146]. Ebenfalls zu bedenken sind die Fälle aus dem Ordnungswidrigkeitenbereich, in welchem die Anwendungsproblematik besonders akut wird, so z. B., wenn es darum geht, ob ein Datenschutzbeauftragter bestellt werden soll (§§ 28, 38 BDSG) oder aber, ob eine Anmeldepflicht (§ 39 BDSG) besteht.

142) Siehe oben, § 5 B I der Arbeit.

143) § 1 III BDSG; ebenso die Landesdatenschutzgesetze (vgl. FN 124).

144) Fälle 28 ("Geburtsdatum"), 29 ("Aprilscherz") und 30 ("Einkaufsgenossenschaft"); sie werden sogleich vorgestellt. Diese insgesamt kleine Zahl dürfte über den wahren Umfang täuschen, wenn man bedenkt, daß man die Fälle auch unter der Rubrik "Pressestrafsachen" fassen könnte. Leider findet man weder in den BKA-Statistiken, noch in den Strafverfolgungsstatistiken eine solche Rubrik.

145) Das Medienprivileg eines Landesgesetzes war in keinem der Fälle tangiert. Nicht berücksichtigt sind die Fälle, in denen die Daten an die Presse weitergegeben wurden.

146) Fall StA Berlin (DuD 1982, 56 = DANA 2/3/1982, 11 f.). Er ist im Anhang abgedruckt.

Als Beispiel aus dem Ordnungswidrigkeitssektor sei hier der Beschluß des OLG Saarbrücken genannt [147], bei dem es im wesentlichen darum ging, zu klären, was unter dem Begriff der "Presse" im Sinne des § 1 III BDSG zu verstehen ist. Das OLG stellte dabei fest, daß vom formellen Pressebegriff auszugehen sei, d. h., nicht Inhalt und Qualität einer Veröffentlichung, sondern allein die Art ihrer Herstellung oder Ausfertigung entscheidend sei. Eine Unterscheidung zwischen "harmlosen Druckwerken" (die nicht unter das saarländische Pressegesetz fallen) und sonstigen Druckwerken lehnt es ab, da dies dem BDSG nicht zu entnehmen sei. Dieser Auffassung ist zuzustimmen, da nur so eine klare und praktikable Abgrenzung möglich ist und dem Grundsatz einer möglichst einheitlichen Auslegung der Rechtsbegriffe genüge getan ist [148].

Die eben erwähnten drei strafrechtlichen Ermittlungsverfahren wurden alle gemäß § 170 II StPO eingestellt. In einem der Verfahren wurde das "Medienprivileg" expressis verbis als Einstellungsbegründung angeführt:

Fall 28 ("Geburtsdatum"):

Nachdem eine Frau gegenüber einer Zeitung wiederholt vergeblich gefordert hatte, ihr Geburtsdatum nicht zu veröffentlichen, stellte sie Strafantrag. Der Staatsanwalt stellte ohne weitere Ermittlungen wenige Tage später das Verfahren mit der Begründung ein, "§ 1 III dieses Gesetzes (BDSG) erklärt sich jedoch ausdrücklich für nicht anwendbar, soweit personenbezogene Daten von der Presse zu publizistischen Zwecken verarbeitet werden." Auch sei keine Straftat nach dem Landespressegesetz ersichtlich.

Der Sachverhalt des zweiten Verfahrens spricht für sich:

147) OLG Saarbrücken NJW 1981, 136 - 137 = DuD 1981, 57.

148) Ebenso O. Mallmann NJW 1981, 137.

Fall 29 ("Aprilscherz"):

Eine Tageszeitung veröffentlichte am 1. April einen satirischen Artikel über den Datenschutz u. den Bundesdatenschutzbeauftragten [149]. Der Anzeigenerstatter argumentierte, "der inkriminierende Artikel zielte direkt darauf ab, schutzwürdige Interessen Dritter, die bereits in einem Bundesland den Rang eines Grundrechts haben, (Nordrhein-Westfalen) lächerlich zu machen". Die Staatsanwaltschaft stellte das Verfahren mangels Tatverdacht ein: Es handele sich um einen Aprilscherz.

Im letzten der drei Verfahren wurden gleich drei Fragen nicht erörtert:

1) Das Problem, ob ein Computerausdruck als Datei im Sinne des § 2 III Nr. 3 BDSG anzusehen ist [150].

2) Die Notwendigkeit, daß es sich um personenbezogene Daten im Sinne des § 2 I BDSG handeln muß, womit höchstens die Inhaber von Einzelunternehmen (Einzelfirmen im Sinne des HGB) Betroffene im Sinne des Gesetzes sind [151].

3) Schließlich wurde das Medienprivileg des § 1 III BDSG überhaupt nicht angesprochen.

Inhalt und Verlauf des Verfahrens lassen sich wie folgt zusammenfassen:

Fall 30 ("Einkaufsgenossenschaft"):

Der Rechtsanwalt einer Einkaufsgenossenschaft erstattete gegen eine GmbH, die eine Hintergrundinformationen liefernde Zeitschrift herausgibt, Strafanzeige und stellte Strafantrag, da ein Computerausdruck aus der EDV-Anlage der Genossenschaft abgedruckt worden war. Er enthielt die Umsatzzahlen, Verkaufsstatistiken, Gewinnspannen etc. von Einzelunternehmen und sonstigen

149) Vgl. zu diesem Zeitungsartikel auch den Bericht in "Film und Recht" Nr. 4/1981 S. 206 und Nr. 6/1981 S. 321.

150) Vgl. dazu weiter oben, § 5 A V 4).

151) Daten über eine OHG sind dagegen nach KG Berlin DB 1980, 1062 nicht "personenbezogen". Anders aber, wenn der Durchgriff auf natürliche Personen gegeben ist: Gallwas in: Gallwas/S/S § 2 RN 6.

Unternehmen. Bei der Vernehmung des verantwortlichen Redakteurs (der zugleich Geschäftsführer der GmbH war), gab dieser seine Quelle nicht preis und verwies auf das Landespressegesetz. Zwar wurde bei der Untersuchung des Verlages der abgedruckte Computerausdruck gefunden, aber es war nicht möglich, zu ermitteln, wer diesen zuvor in Händen hatte, da eine Anzahl identischer Ausdrucke in Umlauf war. So wurde (vier Monate nach Anzeigeneingang) "... das Verfahren wegen Verstosses gegen § 41 BDSG gemäß § 170 II StPO mangels Beweisen eingestellt. Die Veröffentlichung personenbezogender Daten als solche ist nicht strafbar." Auch § 17 II oder § 20 UWG seien nicht verletzt.

Aufgrund der quantitativ (wie qualitativ) recht mageren Ausbeute an Fällen ist ein Urteil über die Wahrscheinlichkeit verweisungsspezifischer Fehler beim Medienprivileg kaum möglich. Immerhin ist die Häufung der nicht erörterten Probleme bei Fall 30 ("Einkaufsgenossenschaft") ein "allgemeines" Indiz für die Schwierigkeiten der Strafverfolgungsbehörden mit den Datenschutzgesetzen.

§ 6

Die personenbezogenen und die offenkundigen Daten in der Auswertung

Die Datenschutzgesetze erfassen in ihren Strafbestimmungen lediglich "personenbezogene Daten, die nicht offenkundig sind" [1]. Damit wird auf zwei Tatbestandsmerkmale abgestellt, die untereinander zwar verknüpft sind, doch ihrerseits selbständige Bedeutung haben. Deshalb wird die mit dem Merkmal "personenbezogene Daten" zusammenhängende Auswertung und die Behandlung durch die Strafverfolgungsbehörden gesondert dargestellt (Abschnitt A). Im Abschnitt B wird die Auswertung zum Problem der Offenkundigkeit von Daten erörtert.

A) Personenbezogene Daten

Untersucht wurde, ob überhaupt personenbezogene Daten erlangt oder weitergegeben wurden. In 155 Verfahren konnte dies unproblematisch angenommen werden. Wenn in vielen Fällen daneben nicht-personenbezogene Daten betroffen waren, so ändert dies nichts, da bei jedem Verfahren zumindest ein personenbezogenes Datum ebenfalls Tatobjekt war. Lediglich vier Verfahren bedürfen einer näheren Erörterung im Hinblick auf das Merkmal "personenbezogene Daten". Der Grund für diese geringe Anzahl dürfte darin liegen, daß es sich um einen sehr weiten und einfach auszulegenden Rechtsbegriff handelt, womit ein Rückgriff auf eine Legaldefinition kaum notwendig wird. Inwieweit die Verweisung auf die Definition [2] gesehen wurde, ließ sich hier

1) § 41 BDSG; ebenso alle Strafbestimmungen der Landesdatenschutzgesetze.

2) Für das BDSG: § 2 I BDSG: "Im Sinne dieses Gesetzes sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)."

deshalb nicht präzise ermitteln. Mögliche Fehler im Hinblick auf die Rechtsanwendung deuten sich nur in den folgenden vier Verfahren an:

Bei zwei Verfahren hätte eine nähere Sachverhaltsaufklärung durch die Staatsanwaltschaften Aufschluß bringen können, inwieweit jeweils Daten von natürlichen oder juristischen Personen betroffen waren:

Im bereits vorgestellten Fall 30 ("Einkaufsgenossenschaft") [3] lagen sowohl Daten von natürlichen Personen (Einzelfirmen), als auch von juristischen Personen vor.

Im anderen Fall waren Computerausdrucke einer Bank gefunden worden. Auf ihnen waren die Kontobewegungen der verschiedensten Konteninhaber verzeichnet.

Die beiden restlichen Verfahren sind durch Subsumtionsfehler gekennzeichnet:

Fall 31 ("Getrenntleben"):

Die Eheleute E lebten getrennt. Frau E besuchte des öfteren ihren Freund F in dessen Wohnung. Herr E kannte von F nur dessen Kfz-Kennzeichen. Der Kriminalbeamte B wurde nun beschuldigt, dem befreundeten Herrn E mit Hilfe des Kfz-Kennzeichens "den Namen, die genaue Anschrift sowie die Beschäftigungsstelle" des F mitgeteilt zu haben. Nach Vernehmung des B als Beschuldigten und des Herrn E als Zeugen wurde das Verfahren Mitte 1981 mit folgender Begründung eingestellt:

"Selbst wenn B den Namen bekanntgegeben haben sollte, erfüllt dies nicht den Straftatbestand des § 41 des Bundesdatenschutzgesetzes, denn gem. § 2 BDSG sind nur solche personenbezogene Daten geschützt, die Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten natürlichen Person beinhalten. Die Bekanntgabe eines Namens oder auch einer genauen Anschrift einer Person erhält keine Angaben, die persönliche oder sachliche Verhältnisse betreffen. Ein hinreichender Tatverdacht für ein strafbares Verhalten des Beschuldigten B ist somit nicht gegeben."

3) § 5 B II der Arbeit.

Obwohl die Staatsanwaltschaft im Fall 31 ("Getrenntleben") die Legaldefinition aus § 2 BDSG heranzog, erkannte sie nicht den Personenbezug von Name und Anschrift.

Fall 7 ("Motorradzulassung"): [4]

Der bei einem Amt der Stadt S angestellte Motorradfahrer M erreichte Mitte März die Zulassung seines (privaten) Motorrades. Zwei Wochen später wurde er von der Verwaltung der Stadt S angeschrieben und um Stellungnahme gebeten, da die Zulassung während der Zeit, in der er als krank gemeldet gewesen sei, geschehen sei.

M erhob daraufhin Dienstaufsichtsbeschwerde und stellte Strafantrag wegen Verstoßes gegen das Landesdatenschutzgesetz in Verbindung mit § 26 V StVZO.

Die Ermittlungen (in die auch der Landesbeauftragte für den Datenschutz eingeschaltet war [5]) ergaben, daß nach einer Anfrage der Stadt an die Zulassungsstelle diese die Daten weitergegeben hatte. Da jedoch weder bei der Zulassungsstelle noch bei der Stadtverwaltung das Anfrage- und/oder Antwortschreiben aufzufinden war, blieb ungeklärt, welche konkreten Personen gehandelt hatten.

Die Dienstaufsichtsbeschwerde wurde mit folgender Begründung abgewiesen:

"Zur Wahrung der Bestimmungen über den Datenschutz sind die Behörden verpflichtet, die Daten sammeln und verwalten. Wenn eine solche Behörde ohne Angabe eines Rechtsgrundes eine Auskunft erteilt, so kann diese nicht dem Auskunftsersuchenden angelastet werden. Das Zulassungsdatum eines Kraftfahrzeuges ist auch kein personenbezogenes, sondern ein fahrzeugbezogenes Datum." Der Landesbeauftragte für den Datenschutz antwortete:

"Wir sehen im Vorgehen der Verwaltung der Stadt S ein Verleiten der Zulassungsstelle zu einer objektiv nicht zulässigen Datenübermittlung." Die Daten seien nicht zur rechtmäßigen Aufgabenerfüllung erforderlich gewesen. Es sei deshalb gegenüber S eine Beanstandung im Sinne des Landesdatenschutzgesetzes ausgesprochen worden.

M zog daraufhin seinen Strafantrag zurück, worauf der Staatsanwalt das Verfahren gemäß § 170 II StPO einstellte, da § 41 Bundesdatenschutzgesetz (alle anderen Beteiligten und auch die Polizei sprachen ständig vom Landesdatenschutzbeauftragten) ein echtes Antragsdelikt sei und daher nach Rücknahme ein Verfahrenshindernis bestehe.

Beim Fall 7 ("Motorradzulassung") ist ein verweisungsspezifischer Fehler der für die Dienstaufsichtsbeschwerde zuständigen Stelle zu vermuten: Hätte sie die Legaldefinition von "personenbezogenen Daten" gelesen, wäre sie eher zu der Auffassung gekommen, daß das "fahrzeugbezogene" Datum der Zulassung hier personenbezogen war, da eine Verknüpfung mit dem Namen des M gegeben war.

4) Der Fall wurde bereits in § 5 A IV der Arbeit kurz angesprochen.

5) Der Landesdatenschutzbeauftragte hat in diesem Bundesland ein uneingeschränktes Strafantragsrecht.

B) Offenkundige Daten

Nach § 41 BDSG wird nur bestraft, wer mit "... Daten, die nicht offenkundig sind, ..." eine der Tatmodalitäten verwirklicht [6]. Diese Einschränkung wurde erst zu einem sehr späten Zeitpunkt in den Gesetzesentwurf mit der Begründung aufgenommen, es handele sich nur um eine redaktionelle Änderung [7].

I) Auswertungsergebnisse

In den vorliegenden 159 Ermittlungsverfahren wäre in 17 Fällen eine Auseinandersetzung mit dem Tatbestandsmerkmal "offenkundig" geboten gewesen. Die Strafverfolgungsbehörden behandelten diese Fälle indessen in unterschiedlicher Weise:

1) Bei neun Verfahren wurde, ohne das Tatbestandsmerkmal "offenkundig" zu benennen, darauf abgestellt, daß die Tatsache bekannt sei oder beschafft werden könne [8].

2) In einem Verfahren ließ die Staatsanwaltschaft die Frage dahinstehen, ob die Adresse offenkundig sei, da die Übermittlung zulässig sei (§ 24 II BDSG) [9]. Nur in diesem Verfahren wurde das Tatbestandsmerkmal "offenkundig" von der Staatsanwaltschaft ausdrücklich in der Begründung der Einstellungsverfügung angesprochen (sieht man von den Fällen ab, in denen einfach der Wortlaut der Strafnormen wiederholt wurde).

6) So auch alle Landesdatenschutzgesetze.

7) BT-Drs. 7/5277 vom 2.6.1976, S. 11 (= "Zu § 32").

8) Vgl. dazu z. B. den in diesem Abschnitt folgenden Fall 35 ("Viehstatistik"). Er ist ausführlich im Anhang dargestellt.

9) Fall 33 ("Reklamesendung"), der in diesem Abschnitt dargestellt wird.

3) Bei sechs Verfahren wurde die sich aufdrängende Frage der Offenkundigkeit von den Staatsanwaltschaften wohl deshalb nicht angesprochen, da sie aus anderen Gründen (fünfmal erfolgte eine Einstellung) abgeschlossen wurden [10].

4) In einem Verfahren schließlich erhob die Staatsanwaltschaft Anklage, das Gericht lehnte jedoch die Eröffnung des Hauptverfahrens ab, da die Daten offenkundig seien [11].

II) Die Auslegung des Begriffs "offenkundig"

Das Tatbestandsmerkmal "offenkundig" ist in den Datenschutzgesetzen nicht definiert. Teilweise wird auf die in den §§ 23 S. 2, 32 I 2 BDSG verwandte Formulierung "unmittelbar aus allgemein zugänglichen Quellen" verwiesen [12], teilweise wird der Begriff "weiter" ausgelegt [13].

Ausgegangen wird meist von der Entscheidung des BGH zu § 244 III StPO, nach der als offenkundig die allgemein bekannten Tatsachen und die gerichtskundigen Tatsachen gelten [14]. Allerdings wird dann nur die Unterdefinition der allgemein bekannten Tatsachen ("solche Vorgänge, von denen verständige Menschen regelmäßig Kenntnis haben oder die sie sich aus zuverlässiger Quelle ohne besondere Fachkunde sicher unterrichten können" [15]) aufge-

10) Vgl. dazu z. B. die im Anhang ausführlich dargestellten Fälle 34 ("Studienfachangabe") und 57 ("Verlobtenfinanzen"). Fall 34 wird hier in diesem Abschnitt kurz angesprochen.

11) Fall 32 ("Bankindiskretion"); Ausführlich im Anhang, hier nur in Kurzfassung.

12) Auernhammer, Kommentar, § 41 RN 1; Ordemann/Schomerus § 32 Anm. 1.; Tiedemann NJW 1981, 950 und wohl auch Hammerbacher DuD 1983, 115.

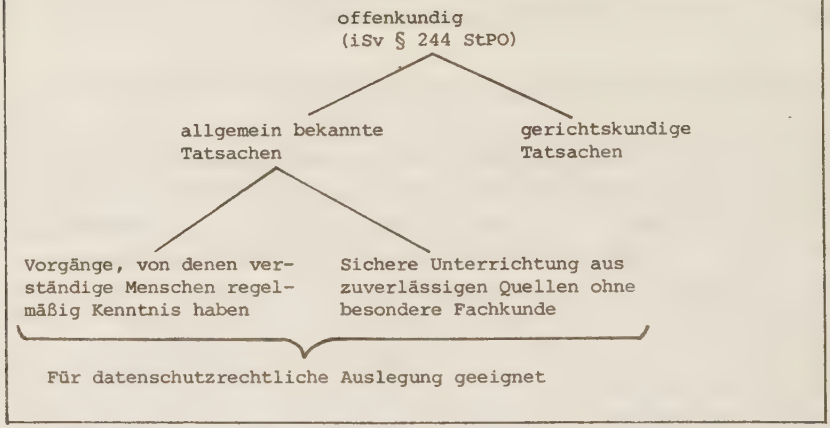
13) So Dammann in: Simitis/D/M/R § 41 RN 6. Schneider in: Gallwas/S/S § 41 RN 31 spricht davon, daß die §§ 23 S. 2 und 31 I 2 BDSG eine "engere Regelung enthalten".

14) BGHSt 6, 292 - 297 = NJW 1954, 1656 f.

15) BGHSt 6, 292, 293 = NJW 1954, 1656; ebenso BGHSt 26, 56, 59.

führt, was verständlich ist, da nur dieser Teil der Offenkundigkeitsdefinition bei § 41 BDSG einen Sinn ergibt. Strukturell läßt sich das Problem in Abbildung 6.1 zeigen:

Abb. 6.1 "Struktur des Begriffs 'offenkundig' ":



Die Übernahme nur eines Teils der Begriffserklärung nämlich der "allgemein kundigen Tatsachen", deutet schon die Schwierigkeiten der Auslegung an [16]. Denn - wie Tiedemann [17] formuliert - im Datenschutz fehlt die prozessuale Beweissituation mit der Trennung von privatem und amtlichem Wissen des Richters [18].

16) Auch der Hinweis auf § 291 ZPO (so z. B. von Kamlah in: Burhenne/Perband § 41 RN 8; Ordemann/Schomerus § 41 Anm. 1.1; Auernhammer, Kommentar, § 41 RN 1; für die Landesgesetze vgl. nur Bautsch Erl. 2 zu § 21 NDSG und Grell Anm. 4. zu § 25 LDSG BW) vermag daran nichts zu ändern.

18) In die gleiche Richtung geht der Vorbehalt von Schneider in: Gallwas/S/S § 41 RN 32; sowie Kamlah in: Burhenne/Perband § 41 RN 8.

Bei der Auslegung des Begriffs "offenkundig" soll zunächst von den beiden Teilen der Unterdefinition von "allgemein bekannte Tatsachen" ausgegangen werden. Dabei ist als erstes zu klären, wie die Formulierung "Unterrichtung aus zuverlässigen Quellen" datenschutzrechtlich zu verstehen ist. Insbesondere stellt sich die Frage, inwieweit eine Verweisung auf die in den §§ 23 S. 2, 32 I 2 BDSG verwandte Formulierung "unmittelbar aus allgemein zugänglichen Quellen" vorliegt ("1) Allgemein zugängliche Quellen und Offenkundigkeit").

Nach dieser verweisungsbezogenen Erörterung soll die mit der Formulierung "Vorgänge, von denen verständige Menschen regelmäßig Kenntnis haben" zusammenhängende Problematik kurz skizziert werden. ("2) Kenntnisse "verständiger Menschen" und Offenkundigkeit").

Zum Abschluß schließlich wird zu untersuchen sein, wie lange eine Tatsache offenkundig ist, d. h., ob einmal offenkundige Tatsachen allein durch Zeitablauf und/oder durch einen bestimmten Akt wieder zu nicht offenkundigen Daten werden können ("3) Länge der Offenkundigkeit"). Diese Fragestellung, die die Dimension der Zeit einbezieht, gilt nicht nur für Daten aus allgemein zugänglichen Quellen, sondern für alle offenkundigen Daten.

1) Allgemein zugängliche Quellen und Offenkundigkeit

Die Problematik, inwieweit Daten aus allgemein zugänglichen Quellen offenkundig sind, läßt sich am besten an Fall 32 ("Bankindiskretion") verdeutlichen:

Fall 32 ("Bankindiskretion"): [19]

Der Betroffene hatte zweimal eine eidesstattliche Versicherung abgeben müssen und es war deswegen auch einmal Haftbefehl erlassen worden. Da die Bank diese Tatsache dem Arbeitgeber des Betroffenen mitgeteilt hatte, erhob die Staatsanwaltschaft Anklage. Das Gericht lehnte jedoch die Eröffnung des Hauptverfahrens ab: "Die Amtsgerichte können jedermann auf Anfrage Auskunft über das Vorliegen von eidesstattlichen Versicherungen und Haftbefehlen einer Person erteilen. Die im vorliegenden Fall übermittelten Daten waren daher offenkundig."

Aus dieser Begründung ist zu entnehmen, daß das Gericht "offenkundig" wohl mit "allgemein ("jedermann") zugängliche Quelle" gleichgesetzt [20]. Zu prüfen ist indessen, ob nicht eine Gleichsetzung mit der Formulierung "unmittelbar aus allgemein zugänglichen Quellen" geboten ist, d. h., ein stillschweigender Verweis des Tatbestandsmerkmals "offenkundig" auf die Formulierung der §§ 23, 32 BDSG anzunehmen ist [21].

Das Problem einer solchen Gleichsetzung liegt im Wort "unmittelbar". Denn verschafft sich der Beschuldigte die Daten nur mittelbar aus einer allgemein zugänglichen Quelle, so z. B., wenn die Bank die Daten sich nicht selbst von dem betreffenden Amtsgericht, sondern über eine Auskunftei beschafft hatte, so fehlte es an der Unmittelbarkeit. Es läge keine Offenkundigkeit vor, der Anwendungsbereich des § 41 BDSG wäre also zunächst eröffnet. Hätte der Beschuldigte dagegen die Daten unmittelbar aus der Schuldnerkartei entnommen, so wären sie bei dieser Interpretation offenkundig. Der Tatbestand des § 41 BDSG wäre damit von vornherein ausgeschlossen.

Da nach dem Wortlaut beide Möglichkeiten bestehen, ist die Auslegung des Begriffs "offenkundig" geboten.

19) Ausführliche Sachverhaltsdarstellung im Anhang.

20) Eine allgemein zugängliche Quelle ist nach der Definition des BVerfG "jede Informationsquelle, die technisch geeignet und bestimmt ist, der Allgemeinheit, d. h. einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen" (BVerfG 27, 71, 83; 33, 52, 65). Hier ist diese "Quelle" das Schuldnerverzeichnis (vgl. § 915 ZPO).

21) Für die Gleichsetzung: Ordemann/Schomerus § 32 Anm.1.; Auernhammer, Kommentar, § 41 RN 1; Tiedemann NJW 1981, 950 und wohl auch Hammerbacher DuD 1983, 115.

Aus den Gesetzesmaterialien ergibt sich, daß zunächst alle personenbezogenen Daten aus dem Schutzbereich des ganzen Gesetzes ausgenommen werden sollten, "soweit sie unmittelbar aus allgemein zugänglichen Quellen entnommen worden sind" [22].

Später wurde diese Passage "im Interesse einer Verstärkung des Datenschutzes gestrichen" [23]. Gleichzeitig wurden die Ausnahmeregelungen der §§ 23 S. 2, 32 I 2 BDSG statuiert und die in die Strafbestimmung aufgenommene Einschränkung "nicht offenkundig" als "redaktionelle Änderung" bezeichnet [24]. Daraus muß geschlossen werden, daß der Gesetzgeber "offenkundig" und "unmittelbar aus allgemein zugänglichen Quellen" als Synonyme verstand.

Aber auch aus Sinn und Zweck der Datenschutzgesetze kann auf eine einschränkende Interpretation des Offenkundigkeitsbegriffes geschlossen werden. Nur die einschränkende Auslegung mit dem Unmittelbarkeitskriterium, d. h. die Daten müssen unmittelbar aus allgemein zugänglichen Quellen entnommen sein, erweist sich als interessengerecht. Dies ergibt sich aus folgenden Überlegungen:

Die in den Datenschutzgesetzen statuierte Herausnahme der offenkundigen Daten aus dem Schutzbereich der Strafbestimmungen birgt die Gefahr in sich, daß auch schwerste Verletzungen der Persönlichkeitsrechte nur deshalb nicht geahndet werden können, da ein Persönlichkeitsprofil [25] aus Mosaiksteinen offenkundiger Daten gebildet wurde [26]. Zwar erscheint jede offenkundige Tatsache

22) BT-Drs. 7/5277 vom 2.6.1976, S. 14 ("§ 2 II").

23) BT-Drs. 7/5277 vom 2.6.1976, S. 5 ("Zu § 1").

24) BT-Drs. 7/5277 vom 2.6.1976, S. 11 ("Zu § 32").

25) Eine (psychologische) Definition des Begriffes gibt Alke DuD 1982, 90.

26) Meister, Datenschutz, S. 28; vgl. dazu auch Goll S. 79/80.

für sich allein betrachtet als "harmlos" und "belanglos", es gibt aber, wie das BVerfG im Volkszählungsurteil zurecht dargelegt, "unter den Bedingungen der automatischen Datenverarbeitung kein "belangeloses" Datum mehr" [27]. Zusammengefügt können auch offenkundige Daten ein genaues Bild ergeben, das um so schärfer und genauer ist, je mehr Informationen über den Einzelnen vorliegen [28]. War die Bedrohung durch solche Mosaikbilder offenkundiger Daten bisher nur in Einzelfällen gegeben, so ändert sich mit Einführung der EDV diese Situation grundlegend [29]: Nunmehr ist es nicht nur möglich, auf schnellere und einfachere Art Daten zu erheben, sondern es ist vor allem möglich, über jeden Einzelnen, technisch gesehen unbegrenzt speicherbare, Datensammlung anzulegen, deren Umfang praktisch beliebig ist und bei denen die Zugriffszeit ohne Rücksicht auf Entfernungen sich nach Sekunden bemißt. Es können damit Persönlichkeitsbilder zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung kontrollieren kann [30]. BKA-Präsident Herold formuliert das so [31]:

"Die Grenzenlosigkeit der Informationsverarbeitung würde es gestatten, das Individium auf seinem gesamten Lebensweg zu begleiten, von ihm laufend Momentaufnahmen, Ganzbilder und Profile seiner Persönlichkeit zu liefern, es in allen Lebensbereichen, Lebensformen, Lebensäußerungen zu registrieren, zu beobachten, zu überwachen und die so gewonnenen Daten ohne die Gnade des Vergessens ständig präsent zu halten. Die Gefahren des "großen Bruders" sind nicht mehr bloß Literatur. Sie sind nach dem heutigen Stand der Technik real."

27) BVerfG NJW 1984, 419, 422; ebenso: Egloff ZSR 96 (1977) I S. 351; Heussner, FS Wannagat, 1981 S. 175; Mallmann/Walz NJW 1981, 1022; Schünemann ZStW 90 (1978) S. 24 FN 36; vgl. auch Simon/Taeger JZ 1982, 141; dies., Rasterfahndung, S. 45.

28) Simon/Taeger, Rasterfahndung, S. 39; Rissing-van Saan S. 73 mwN.

29) BVerfG NJW 1984, 419, 421; vgl. auch Herden/Karrer VOP 1981, 366.

30) BVerfG NJW 1984, 419, 421. Zu Beispielen aus den USA vgl. O. Mallmann, Zielfunktionen, S. 58.

31) Herold, RuP 1980, 81; ähnlich Rissing-van Saan S. 114; Tubies DuD 1979, 75 und der (neue) BfD, R. Baumann ÖVD 1983, 108.

Durch die Verbreitung automatischer Datenverarbeitungsanlagen werden immer mehr "offenkundige" Daten elektronisch gespeichert. Bereits jetzt können, um nur einige Beispiele zu nennen, folgende Verhaltensweisen in Datenverarbeitungsanlagen festgehalten werden: Die Geldabhebung mittels Scheckkarte, die Ausleihe von Büchern, der Zu- und Abgang in Betrieben und Behörden, die Art und Weise der Btx-Benutzung [32], Reisebuchungen [33] sowie die Telefoniergewohnheiten [34]. Ferner sind schon heute auf öffentlichen Straßen und Plätzen sowie z. B. in Kaufhäusern zahlreiche Fernsehkameras installiert, die die Möglichkeit der unbegrenzten und unkontrollierten Sammlung offenkundiger Daten geben. Da es bereits in Ansätzen technisch realisierbar ist, daß Computer Bilder erkennen und zuordnen können, bestände somit die Möglichkeit einer automatischen Erkennung von Personen, etwa anhand des über jeden bestehenden Paßbildes [35]. Würde nun nach Erkennung eine Speicherung und Zusammenführung aller Daten erfolgen, so könnte ein "Bewegungsprofil" eines jeden einzelnen angelegt werden. Wenn man nun noch die Verknüpfung mit den in anderen Datensammlungen gespeicherten nichtoffenkundigen Daten durchführt, erhält man ein vollständiges Persönlichkeitsprofil und die Gefahr des "Gläsernen Menschen"

32) Zur Registrierung des über Btx ablaufenden Konsumverhaltens: Bull DuD 1982, 151 und DANA 3/4/1983 S. 19. Zu den "unerschöpflichen Möglichkeiten" Persönlichkeitsprofile herzustellen: Bartl, Handbuch-Btx-Recht, RN 199 (S. 177).

33) Zum Problem "Reisebüro und BDSG": Laduga DuD 1978, 204 ff.

34) Vgl. dazu den im Anhang vorgestellten Fall 39 ("Telefondatenerfassung"). Aus der Rechtsprechung dazu: BVerwG NJW 1982, 840; OVG Bremen DuD 1980, 104; LAG Frankfurt MDR 1982, 82.

35) Nach einem Bericht der "computer zeitung" vom 18.1.1984, S. 24, hat die Wiener Polizei zusammen mit IBM Austria ein vollelektronisches Fahndungssystem entwickelt, mit dessen Hilfe Phantombilder mit gespeicherten Fahndungsfotos verglichen und erkannt werden können.

Zur Forschung bezügl. sog. "bildverstehender Systeme" vgl. die Berichte im "computer magazin" Heft 7/8 1983, S. 42 ff. u. 54 ff.

wird Wirklichkeit. Bull legt zurecht dar, daß "sich viele noch nicht klar machen", was eine "total durchsichtige Welt" bedeutet und führt aus [36]:

"Wer da meint, er habe "sich nichts zuschulden kommen lassen", der verkennt, daß es zu den bisher nie gefährdeten existentiellen Bedingungen des sozialen Zusammenlebens gehört, in verschiedenen Rollen (als Berufstätiger, Familienvater, Gläubiger, Parteimitglied, Verbandsvertreter usw.) und dabei auch in Widersprüchen leben zu können. Die Gefahr, daß diese Freiheit verloren geht, wird durch Technik allein nicht begründet, aber die Technik wirkt als Trendverstärker."

Sinn und Zweck der Datenschutzgesetze ist der Schutz des Einzelnen vor der Datenverarbeitung. Dies ist aber nur möglich, wenn alle Daten, also selbst belanglose, wozu auch offenkundige zählen, geschützt werden [37]. Angesichts des Wortlauts der gegenwärtigen Strafbestimmungen ist indessen das Ziel eines umfassenden Schutzes aller personenbezogener Daten nur über eine restriktive Auslegung des Tatbestandsmerkmals "offenkundig" zu erreichen [38]. Damit ist zu fordern, daß die Daten "unmittelbar" aus allgemein zugänglichen Quellen entnommen sein müssen. Nur diese Daten unterliegen dann nicht dem Schutz der Strafbestimmungen.

Die Konsequenz dieser Auslegung bedeutet für Fall 32 ("Bankindiskretion") [39], daß hier eine weitere Sachverhaltsaufklärung geboten gewesen wäre, um festzustellen, woher die Bank die Daten erhalten hatte. Nur wenn sie die Daten unmittelbar aus dem Schuldnerverzeichnis entnommen hätte, wäre § 41 BDSG von vornherein ausgeschlossen gewesen.

36) Bull, Ziele und Mittel, S. 15 f.

37) Nach Simon/Taeger JZ 1982, 141 sind selbst die "harmlosesten" Informationen vor jeglichem Erheben zu schützen.

38) Für eine restriktive Auslegung ist auch Schneider in: Gallwas/S/S § 41 RN 33.

39) Siehe oben, § 6 B II 1).

Das Problem der offenkundigen, d. h. unmittelbar aus allgemein zugänglichen Quellen entnommenen Daten stellt sich in gleicher Weise bei den sog. Adressenfällen [40], denn regelmäßig läßt sich hier die Adresse aus Telefon oder Adressbüchern entnehmen. Dazu folgendes Verfahren:

Fall 33 ("Reklamesendung"):

Frau F bekam seit ca. 1 Jahr Reklamesendungen. Als sich darunter Kataloge mit Sexartikeln befanden, erstattete sie Strafantrag "wegen Verstoßes gegen das Datenschutzgesetz". Sie fühle sich durch diese Angebote beleidigt und habe niemals ihre Zustimmung zur Weitergabe ihrer Anschrift gegeben. Der von der Staatsanwaltschaft ermittelte Absender, ein Gummiwarenfabrikant, verweigert die Aussage. Die Staatsanwaltschaft stellte das Verfahren ein: "Die Adresse und der Name der Anzeigenerstatterin sind offenkundig, da sie für jeden ohne weiteres aus Telefon- oder Adressbüchern zu ersehen sind." F erhob Beschwerde, da sie unter ihrem Namen weder in Telefon- noch Adressbüchern benannt sei. Der Generalstaatsanwalt führte darauf in seinem Bescheid aus: "Die Frage, ob die Daten "offenkundig" sind, kann dahinstehen. Es handelt sich um den üblichen Adressenhandel. Die Übermittlung ist zulässig und es besteht kein Grund zur Annahme, daß schutzwürdige Belange beeinträchtigt sind (§ 24 II BDSG). Im vorliegenden Fall ist die Grenze des Zulässigen nicht überschritten worden." Soweit sie sich beleidigt fühlte, hätte sie Strafantrag wegen Beleidigung stellen müssen.

Das Verfahren wurde hier zurecht eingestellt. Einer näheren Sachverhaltsaufklärung bedurfte es nicht. Folgt man der hier vertretenen engen Auslegung des Begriffs "offenkundig", so wäre das Verhalten von vornherein nur dann nicht in den Schutzbereich des § 41 BDSG gefallen, wenn der Beschuldigte die Daten "unmittelbar" aus allgemein zugänglichen Quellen entnommen hätte. Bei einer nur mittelbaren Erlangung der Daten (über den Adressenhandel z. B.) wäre zwar § 41 BDSG grundsätzlich anwendbar gewesen, da aber die rechtfertigenden Voraussetzungen des § 24 II BDSG vorlagen, hätte man ebenfalls einstellen müssen. Dies gilt selbst für den Fall, daß die Behauptung der Frau, sie sei weder im Telefon- noch Adressbüchern gespeichert, zutreffend gewesen sein sollte.

40) D. h. der Handel mit Adressen. Vgl. dazu die Regelung des § 24 II BDSG. Bei rund einem Viertel der Fälle waren primär Adressen betroffen.

2) Kenntnis "verständiger Menschen" und Offenkundigkeit

Bei Daten, die weder mittelbar noch unmittelbar aus allgemein zugänglichen Quellen entnommen sind, liegt die Auslegungsschwierigkeit in der Frage, was unter "regelmäßige Kenntnis verständiger Menschen" zu verstehen ist. Es ist also primär ein Problem der Auslegung und nicht von Verweisungen. Dennoch sollen zwei Verfahren vorgestellt werden, anhand derer die Auslegungsfrage deutlich wird:

Fall 34 ("Studienfachangabe"): [41]

Eine Universität hatte verschiedene Daten von Studenten an eine GmbH weitergegeben. Die Staatsanwaltschaft war der Meinung, daß "die Angabe des Studienfaches bei dem einzelnen Studenten als letztlich öffentlich bekanntes Merkmal anzusehen" sei.

Fall 35 ("Viehstatistik"): [42]

Der Bürgermeister einer kleinen Gemeinde wurde beschuldigt, Daten aus einer Viehstatistik unbefugt verwandt zu haben. Zur Begründung der Einstellung zitierte die Staatsanwaltschaft die Behauptung des Beschuldigten: "Im Ort ist unter Landwirten allgemein bekannt, wieviele Schweine in den einzelnen Betrieben gehalten werden."

Bei diesen zwei Verfahren sind personenbezogene Daten betroffen, die nicht aus allgemein zugänglichen Quellen stammen und darüberhinaus lediglich einem bestimmten Personenkreis bekannt sind. Das Studienfach eines Studenten ist zwar dessen Verwandten, Bekannten und Freunden bekannt, nicht aber jedem verständigen Menschen. Gleiches gilt für die Zahl der Schweine im Fall 35 ("Viehstatistik").

41) Ausführliche Falldarstellung im Anhang.

42) Ausführliche Falldarstellung im Anhang.

Es kann davon ausgegangen werden, daß grundsätzlich alle personenbezogenen Daten einem mehr oder minder großen Kreis von Personen bekannt sind. Die Daten sind dann für diesen Personenkreis frei verfügbar, sie können beliebig verwertet werden. Fraglich ist, ob sie damit auch für eine Verarbeitung in DV-Anlagen frei verfügbar sind. Dies kann man aufgrund des Sinn und Zwecks der Datenschutzgesetze indessen nicht annehmen. Es ist wiederum auf das Urteil des BVerfG hinzuweisen, wonach es unter den Bedingungen der automatischen Datenverarbeitung kein "belangloses" Datum gibt [43]. Somit ist also auch hier (wie oben dargelegt [44]) eine restriktive Auslegung geboten. Deshalb sind Daten nur dann als"offenkundig" anzusehen, wenn sie für jeden verständigen Menschen offenkundig sind, wie z. B. die Namen und sonstigen Daten von Politikern oder sonst im öffentlichen Leben stehenden Personen. Mit anderen Worten: Daten, die nicht jedem verständigen Durchschnittsmenschen bekannt sind, müssen so behandelt werden wie alle anderen personenbezogenen Daten und können somit prinzipiell Gegenstand einer strafbaren Handlung sein.

Wendet man dieses Auslegungsergebnis auf die obigen Verfahren an, so zeigt sich, daß bei allen Verfahren die Daten nicht "jedem" bekannt und somit nicht offenkundig waren. Den Staatsanwaltschaften kann indessen hier nicht vorgehalten werden, verweisungsspezifische Fehler begangen zu haben, da es sich um ein reines Auslegungsproblem handelt.

3) Länge der Offenkundigkeit

Das letzte Auslegungskriterium im Hinblick auf den Begriff "offenkundig" bezieht die Dimension der Zeit mit ein. Es ist zu klären, wie lange eine Tatsache offenkundig ist, d. h., werden einmal offenkundige Daten allein durch Zeitablauf und/oder durch einen bestimmten Akt wieder zu nicht offenkundigen Daten?

43) BVerfG NJW 1984, 419, 422.

44) Siehe eben, § 6 B II 1).

Diese Problematik soll an einem aus dem Jahre 1983 stammenden Fall [45] verdeutlicht werden:

Fall 100 ("Nachnahmelieferung"):

Die Anzeigenerstatterin A bestellte Anfang 1983 beim Zeugen Z Waren im Wert von 700,-- DM. Nachdem dieser zweimal die Ware per Nachnahme (wie im Kaufvertrag vereinbart) vergeblich hatte zustellen lassen (jedes Mal wurde die Annahme verweigert), wandte er sich Ende Oktober 1983 an die beschuldigte Handelsauskunftei H. Diese teilte ihm mit, daß nach ihren Unterlagen in der Schuldnerkartei des Amtsgerichts ein Haftbefehl vom Juni 1980 zur Erlangung einer eidesstattlichen Versicherung eingetragen sei. Die Tatsache, daß diese Eintragung nach Nachweis der Zahlung durch die A im August 1980 gelöscht worden war, wurde ihm nicht mitgeteilt. Die A erfuhr von dieser (falschen) Auskunft, und nach Schriftwechsel mit der Aufsichtsbehörde stellte sie rechtzeitig Strafantrag gegen Unbekannt.

Nach Abs. 4 des § 915 ZPO dürfen Abschriften aus dem Schuldnerverzeichnis erteilt werden (nähere Regelung in den allgemeinen Vorschriften (AV) des Bundesjustizministeriums) [46], sofern die Einhaltung der in Abs. 2 des § 915 ZPO vorgesehenen Löschungsfrist gesichert erscheint.

Hier nun hätte die Auskunftei H, die nach § 1 Satz 2 AV als vertrauenswürdiges Unternehmen Abschriften und nach § 1 Satz 5 AV auch von vorzeitigen Löschungen Kenntnis erhält [47], nach erfolgter Befriedigung des (früheren) Gläubigers die Eintragung löschen müssen. Sie hat dies nicht getan, sondern dem Z die alte Lage bekanntgegeben. Es war daher zu prüfen, ob die Verantwortlichen deshalb strafrechtlich [48] zur Rechenschaft gezogen werden konnten. Dabei ergab sich das oben angeschnittene Problem:

45) Das Verfahren konnte deshalb nicht in die Gesamtauswertung einbezogen werden.

46) Allgemeine Vorschriften des Bundesministers der Justiz vom 1.8.1955, BAnz Nr. 156.

47) Gemäß § 1 Satz 6 AV erhält die Auskunftei Kenntnis spätestens bis zum zehnten des auf die vorzeitige Löschung folgenden Monats.

48) Eine andere - wahrscheinlich wirksamere - Sanktionsmöglichkeit wäre der Widerruf der Bewilligung zur Erteilung von Abschriften nach § 8 S. 3 AV.

Wird die einmal offenkundige Tatsache (des Verfahrens zur Abnahme einer eidesstattlichen Versicherung) dadurch zur nicht mehr offenkundigen, daß die Löschung im ursprünglichen Speicherort erfolgte oder aber bleiben einmal offenkundige Daten immer offenkundig im Sinne der Strafbestimmungen der Datenschutzgesetze?

Eine vollständige Lösung der Frage, ob nach Ablauf einer bestimmten Frist, oder nach dem Akt der Löschung die Daten als nicht mehr offenkundig gelten, führt ins Verfassungsrecht, da sich Informationsfreiheit und Meinungsäußerungsfreiheit auf der einen und Persönlichkeitsrecht auf der anderen Seite gegenüberstehen. Wie Kamlah zurecht darlegt [49], ist das Verhältnis Datenschutz und Informationsfreiheit bis heute "ausgeklammert" worden. Da die Lösung dieses einerseits verfassungsrechtlichen und andererseits nicht verweisungsspezifischen Problems nicht Sinn und Zweck der Arbeit ist, sollen hier deshalb nur einige Anmerkungen erfolgen:

Das Persönlichkeitsrecht des Einzelnen kann in bestimmten Fällen überwiegen und der Informationsfreiheit vorgehen (wie die Lebach-Entscheidung des BVerfG [50] zeigt), womit es grundsätzlich möglich sein muß, daß bestimmte Informationen zu nicht mehr offenkundigen erklärt werden können. Der Gedanke einer grundsätzlichen Löschungspflicht [51] für Daten nach Ablauf einer gewissen Zeit ergibt sich aus einer Vielzahl von

49) Kamlah, DVD-Jahrestagung 1979, S. 187.

50) BVerfGE 35, 202 ff.; zustimmend Bull, Ziele und Mittel, S. 42.

51) Brödner S. 157; Bull, Ziele und Mittel des DS, S. 16; Datenschutzkommission des Deutschen Juristentages S. 46; Louis RN 13 und 130; Heussner FS Wannagat S. 179; Baum FuR 4/1979 S. 216; O. Mallmann, Zielfunktionen, S. 125, 130 (für Auskunfteien).

Einzelregelungen, die heute schon bestehen, so etwa die Tilgungsfristen im Bundeszentralregister [52], im Verkehrsregister [53] oder der Schuldnerkartei [54]. Bei einer Novellierung des BDSG und bei bereichsspezifischen Gesetzen sollte deshalb auch das "programmierte Vergessen" [55] beachtet werden. Da jedoch diese Entscheidungen so wesentlich für das Verfassungsverständnis sind, müssen sie den Parlamenten vorbehalten bleiben. Es ist deshalb durch Gesetze (und nicht durch Verordnungen [56]) zu regeln, welche Daten wann und von wem nach welcher Frist gelöscht werden müssen. Hier ist dann auch an Sonderregelungen für die Presse zu denken.

52) §§ 43 ff. des Gesetzes über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz - BZRG) vom 22.7.1976 (BGBl. I S. 2005).

53) § 29 StVG und § 13 a StVZO.

54) § 915 II ZPO.

55) So Herold, RuP 1980, 84 und Louis RN 130.

56) Die KpS-Richtlinien (dazu Ringwald, INPOL und StA, § 1 III (S. 39)) sollten deshalb vom Parlament "in Gesetzesform gegossen" werden.

§ 7

Auswertung zum Problem der Tatmodalitäten

Nach § 41 BDSG macht sich strafbar, wer personenbezogene Daten unbefugt

- übermittelt,
- verändert,
- abruft oder
- sich aus in Behältnissen verschlossenen Dateien verschafft.

Darüberhinaus ist in den nur im öffentlichen Bereich geltenden Landesdatenschutzgesetzen von Bremen und Schleswig-Holstein das unbefugte "Speichern" und "Löschen" strafbewehrt, in Niedersachsen nur das "Löschen" [1]. In Rheinland-Pfalz muß auch der mit Sanktionen rechnen, der die Daten "sonstwie verwendet" oder wer "den Zugriff auf ... Daten gewährt" [2].

Legaldefinitionen gibt es nur für die Begriffe "Übermittlung", "Veränderung", "Speicherung" und"Löschung" [3], womit lediglich hier verweisungsspezifische Fehler auftreten konnten.

Auswertungsgrundlage stellten die 100 Fälle dar, in denen

1) § 30 I Nr. 1 BrDSG; § 23 I Nr. 1 LDSG SH; § 21 I Nr. 1 NDSG.

2) § 27 I Nr. 1 und 3 LDAtG RP. Die "unbefugte Verwendung" war bereits als § 15 III im LDatG RP vom 24.1.1974 (GVBl. S. 31 f.) enthalten (vgl. oben, § 2 A III). Unter das (jetzige) Merkmal "sonstwie verwendet" fällt nach Kutzmann (Erl. 3 zu § 27) das Speichern für eigene Zwecke und das Löschen; mit der Formulierung "den Zugriff auf ... Daten gewährt" sollen Daten bereits im Vorfeld der Datenverarbeitung geschützt werden (aaO).

3) So in § 2 II BDSG und in den entsprechenden (und insoweit inhaltsgleichen) Landesdatenschutzgesetzen.

Speicherort ("Quelle") eine EDV-Anlage oder eine Kartei waren[4].

Dabei wird im Abschnitt A zunächst eine Auswertung nach der faktischen Relevanz der einzelnen Tatmodalitäten vorgenommen, bevor im Abschnitt B die jeweiligen Tatmodalitäten gesondert interpretiert und hinsichtlich verweisungsspezifischer Fehler analysiert werden.

A) Die faktische Relevanz der einzelnen Tatmodalitäten

Vor einer Auslegung und Analyse der einzelnen Tatmodalitäten soll deren Häufigkeitsverteilung dargelegt werden. Es erschien mir wichtig zu zeigen, welche Tathandlungen in der Praxis einerseits überhaupt vorkamen und andererseits in welcher Anzahl. Gerade im Strafrecht ergeben sich, besonders durch die unterschiedlichen Beteiligungsformen, vielfältige Kombinationsmöglichkeiten. Damit festgestellt werden konnte, welche Tatmodalitäten in den vorliegenden Ermittlungsverfahren besonders häufig auftraten, und denen damit bei der Interpretation besonderes Gewicht beizumessen war, wurde die faktische Relevanz der Handlungen und Handlungsvarianten untersucht. Folglich wurde für jeden Fall zunächst die charakteristische Vorgehensweise festgestellt, wobei einerseits unterschiedliche Tatmodalitäten, andererseits mehrere Täterkonstellationen zu berücksichtigen waren.

4) Die "Nicht-Datei-Fälle" (vgl. oben, § 5 A III) wurden nicht einbezogen. Einerseits erschien es wenig sinnvoll, "Tatmodalitäten" zu untersuchen, obwohl die Handlung schon nicht in den Schutzbereich der Strafnormen fiel. Andererseits war bei der Erarbeitung des Fragebogens davon ausgegangen worden, daß nur wenige Verfahren keinen "Dateibezug" hatten; die hohe Anzahl der "Nicht-Dateien" (beinahe ein Viertel, siehe oben, Tab. 5.1 "Speicherort ("Quelle")", § 5 A II) überraschte. Zum Begriff "Speicherort" siehe oben, § 5 A I. Die 100 Speicherorte setzen sich aus 61 EDV-Anlagen (siehe oben, § 5 A IV) und 39 Karteien (siehe oben, § 5 A V, Tab. 5.5 "Graubereich") zusammen. Da in einem Verfahren mehrere Speicherorte möglich waren (vgl. oben, § 5 A II) stehen hinter diesen 100 Speicherorten 95 Ermittlungsverfahren; weil indessen von der Tatmodalität im Hinblick auf den jeweiligen Speicherort (EDV-Anlage, Kartei) auszugehen war, wurde von 100 Fällen ausgegangen.

Die Festlegung auf ein jeweils bestimmtes Begriffsverhältnis der einzelnen Tatmodalitäten wurde dabei vermieden. Denn die Auswertungsergebnisse wären damit von der Auslegung der Tatbestandsmerkmale abhängig und somit nur beschränkt aussagekräftig gewesen. Wie beim Dateibegriff sollte zunächst eine Klassifizierung der praktisch vorkommenden Handlungen vorgenommen werden [5]. Basierend auf dieser rechtstatsächlichen Einteilung konnten dann die einzelnen Tatbestandsmerkmale interpretiert sowie hinsichtlich Verweisungsfehlern der Strafverfolgungsbehörden analysiert werden.

Um den Schwerpunkt der Tathandlung in der Praxis festzustellen, wurde auf die Sicht des Opfers, des Betroffenen, abgestellt. Sein Vorwurf, der Beschuldigte sei in bestimmter Weise mit seinen Daten verfahren, wurde als Maßstab genommen. In den Fällen, in denen keine Betroffenenäußerung vorlag, wurde eine hypothetische Beurteilung versucht.

Grundsätzlich lassen sich - bezogen auf die Tatmodalitäten - zwei Arten des Vorwurfs unterscheiden: Zum einen die Fälle, in denen der Beschuldigte nur eine bestimmte Modalität verwirklicht haben soll, zum anderen die Fälle, in denen ein ganzer Handlungsablauf der Gegenstand einer Anschuldigung war. Die Auswertung ergab die in Tabelle 7.1 "Handlungsvarianten" dargestellte Klassifizierung der angeblich begangenen Tatmodalitäten:

5) Dazu oben, § 5 A I der Arbeit.

Tabelle 7.1 "Handlungsvarianten":		
1) Übermittlung ("Weitergabe")		22
2) Datenabruf ("Einsicht")		20
3) Sich aus in Behältnissen verschlossenen Dateien verschaffen		1
4) Speicherung		7
5) Löschung		1
6) Abruf und dann Übermittlung		23
7) Abruf u. Übermittlung und Übermittlung		13
8) Speicherung und Übermittlung		13
A l l e F ä l l e	=	100

Erläuterungen zur Tabelle 7.1:

1) Übermittlung ("Weitergabe"):

Hierunter wurden die Fälle gefaßt, in denen der Betroffene dem Beschuldigten vorwarf, die Daten an einen anderen übermittelt ("weitergegeben") zu haben.

2) Datenabruf ("Einsicht"):

Darunter fallen die Verfahren der Datenbeschaffung, sei es durch Abruf oder Einsichtnahme.

3) Sich aus ... verschlossenen Dateien verschaffen:

Hierunter wurden die Fälle gezählt, in denen dem Beschuldigten vorgeworfen worden war, er habe sich die Daten aus verschlossenen Behältnissen beschafft.

4) Speicherung:

Der Betroffene warf hier dem Beschuldigten die unberechtigte Speicherung seiner Daten vor.

5) Löschung:

Die Anschuldigung hatte eine unbefugte Löschung von Daten zum Gegenstand.

6) Abruf und dann Übermittlung:

Dem Beschuldigten wurde vorgeworfen, sich die Daten durch Einsichtnahme beschafft und dann einem anderen weitergegeben oder weitererzählt zu haben.

7) Abrufen und Übermittlung und Übermittlung:

Auch hier soll sich der Beschuldigte die Daten durch Einsicht beschafft und dann weitergegeben haben. Der, an den die Daten gelangten, soll sie daraufhin wiederum einer weiteren Person übermittelt haben.

8) Speicherung und Übermittlung:

Der Betroffene beschuldigte hier einen anderen, Daten über ihn gespeichert und weitergegeben zu haben.

B) Interpretation und Analyse der einzelnen Tatmodalitäten

Im folgenden Abschnitt werden die einzelnen Tatmodalitäten jeweils gesondert analysiert und - soweit Verweisungen vorliegen - danach untersucht, ob und inwieweit verweisungsspezifische Fehler durch die Strafverfolgungsbehörden begangen wurden.

I) Abrufen

Bevor Daten weitergegeben werden können, muß der Beschuldigte von ihnen in der Regel erst Kenntnis erlangen. Es wird deshalb zunächst der "Datenabruf" erörtert [6].

6) Zum Datenabruf ausführlich Ringwald JZ 1983, 291 ff. und ders., INPOL und StA, § 3 (S. 65 ff.).

Das Merkmal "abrufen" führt nach Ringwald [7], "im Gegensatz zur Praxis ... in der Datenschutzliteratur ein gar kümmerliches Dasein". Der Datenabruf werde "mehr vage denn konkret beleuchtet" [8]. In den Datenschutzgesetzen ist der Begriff nicht legaldefiniert, womit insoweit auch keine Verweisung vorliegt. Einen Anhaltspunkt bietet lediglich eine Formulierung in § 2 II Nr. 2 BDSG, wonach auch eine Übermittlung vorliegt, wenn Daten "zur Einsichtnahme, namentlich zum Abruf bereitgehalten werden" [9]. Somit ist der Datenabruf ein Unterfall der Einsichtnahme. Da indessen die Strafbestimmungen nur das unbefugte Abrufen pönalisieren, ist lediglich diese spezielle Art der Einsichtnahme mit Sanktionen bedroht. Zu untersuchen war daher, inwieweit die Strafverfolgungsbehörden diese gesetzliche Wertung, die gleichsam verweisungsähnlich ist, gesehen haben.

1) Fraglich ist jedoch zunächst, ob nur dann ein "Abruf" vorliegt, wenn die Daten durch technische Mittel entnommen worden sind [10], also z. B. nur die über Terminal stattfindende Abfrage aus EDV-Anlagen erfaßt wird, nicht dagegen die aus Karteien.

Dehnt man den Wortlaut aus, so kann man z. B. auch die Kenntnisnahme aus einer Kartei als Datenabruf qualifizieren. Geht man hingegen von der natürlichen Wortbedeutung aus, so wird die Einsicht in eine Kartei nicht mehr erfaßt. Da sich Strafnormen an die Allgemeinheit richten, ist von deren Wortbedeutungsverständnis auszugehen.[11] Damit ist aber die Einschrän-

7) Ringwald, INPOL und StA, § 3 I. 1.a), (S. 65).

8) Ringwald, INPOL und StA, § 3 I. 1.a), (S. 65).

9) Ebenso die Landesdatenschutzgesetze.

10) Kutzmann, Erl. 3 zu § 27 LDatG RP; Arbeitskreis Teil II S. 28; Ordemann/Schomerus § 41 Anm. 1.2.3.; wohl auch Hunsche in: Ruckriegel u. a., Kommentar, Erl. 5 zu § 33 LDSG NW.

11) Baumann AT § 13 I. 3. (S. 154); vgl. auch die Nachweise bei FN 34 in § 3 A der Arbeit.

kung auf die Entnahme von Daten aus EDV-Anlagen durch technische Mittel geboten [12]. Auch die gesetzgeberische Qualifizierung des Abrufens als Unterfall der Einsichtnahme deutet auf dieses Begriffsverständnis hin. Folge dieser Auslegung ist allerdings, daß z. B. die Kenntnisnahme von Daten aus Karteien (die ja auch Dateien darstellen) nur über die Tatmodalität "sich verschaffen aus in Behältnissen verschlossenen Dateien" bestraft werden kann.

In 56 Ermittlungsverfahren wurde dem Beschuldigten (zumindest auch) ein unbefugter Datenabruf vorgeworfen. Davon wurde in fünf Fällen von den Strafverfolgungsbehörden erörtert, inwieweit der Abruf mittels technischer Mittel erforderlich sei. Bei allen fünf Verfahren bejahten die Staatsanwälte dieses Erfordernis; sie beriefen sich dabei zumeist auf die Meinungen der Kommentare von Auernhammer und Ordemann/Schomerus [13].

So führte der Staatsanwalt im Fall 36 ("informatorische Anfrage") [14] in der Einstellungsbegründung aus:

"... scheidet eine Strafverfolgung ... aus, da die Auskunft auf Grund einer schriftlichen Anfrage erfolgte und die Daten nicht im technischen Sinne abgerufen worden sind."

Bei allen anderen Verfahren wurde diese Problematik nicht erörtert. Man konnte im Gegenteil den Eindruck haben, daß das Merkmal "abrufen" eher umgangssprachlich als datenschutzspezifisch verstanden wurde. Die Untersuchung nach Synonymen ergab aber kein Überwiegen eines bestimmten Begriffes. So kamen vor: "anfragen, erfragen, (telefonisch) Auskunft einholen, besorgen, einsehen, verschaffen, beschaffen".

12) Kutzmann Erl. 3 zu § 27 LDatG RP; Arbeitskreis Teil II S. 28; Ordemann/Schomerus § 41 Anm. 1.2.3.

13) Ordemann/Schomerus § 41 Anm. 1.2.3; Auernhammer, Kommentar, § 4 1 RN 2.

14) Ausführliche Falldarstellung im Anhang.

2) Im Laufe der Auswertung wurde zudem ein spezifisch strafrechtliches Auslegungsproblem sichtbar, nämlich die Frage, ob die Modalität des "Abrufens" ein eigenhändiges Delikt darstellt. In einigen Fällen behaupteten dies die Anwälte der Beschuldigten. Die Staatsanwaltschaften indessen lehnten es ab, "abrufen" als eigenhändiges Delikt anzusehen. So führte der Staatsanwalt in Fall 37 ("Bankauskunft") [15] aus:

"§ 41 I Nr. 1 BDSG ist kein eingenhändiges Delikt, weil kein unmittelbar körperlich zu vollziehender Akt notwendig ist. Es ist auf die ähnlich gelagerte Vorschrift des § 203 StGB zu verweisen, die auch kein eigenhändiges Delikt ist."

Diesen Ausführungen ist zuzustimmen. Abgesehen davon, daß eine generelle Zielsetzung bestehen sollte, eigenhändige Delikte abzuschaffen [16], setzt ein Abrufen keine persönliche Ausführungshandlung voraus. Entscheidendes Gewicht ist der Sicht des Opfers, d. h. des Betroffenen, beizumessen. Im Vordergrund steht für das Opfer nicht, wer agiert hat, sondern nur, daß eine Handlung vorgenommen worden ist. Die Verletzung an sich soll verhindert werden, nicht aber die durch einen bestimmten Täter [17]. Da dies beim Datenabruf der Fall ist, liegt kein eigenhändiges Delikt vor.

3) Eine weitere problematische Auslegungsfrage ist, ob der unbefugte Datenabruf eines bei der speichernden Stelle Beschäftigten strafbar ist [18]. Ruft z. B. ein Sachbearbeiter über Terminal aus einer EDV-Anlage solche Daten ab, auf die

15) Ausführliche Falldarstellung im Anhang.

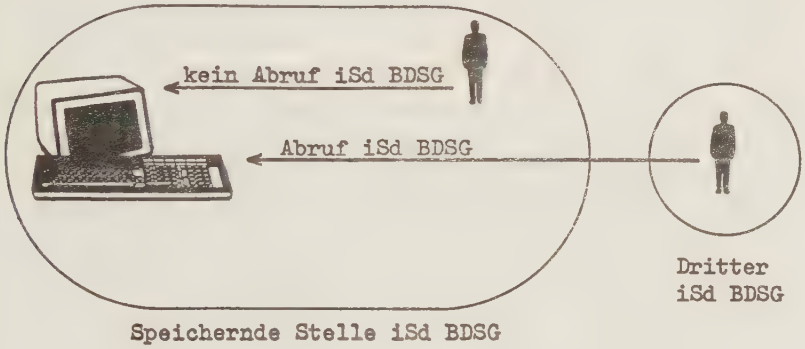
16) So Haft JA 1979, 658 und Auerbach S. 145.

17) Schall JuS 1979, 109.

18) Dazu Ringwald, INPOL und StA, § 3 I. 2. (S. 66 ff.) und § 9 I. 1. a), (S. 171 f.).

er nach seinem Arbeitsvertrag bzw. Anstellungsverhältnis zugreifen darf, so liegt - unbestritten - ein Datenabruf im technischen Sinne vor. Nach Ringwald soll dieser technische Datenabruf nun nicht identisch mit dem Datenabruf im Sinne des BDSG sein [19]. Der "datenschutzrechtliche" Abruf sei enger als der technische. Der Grund dafür ist, daß die Datenschutzgesetze zwischen speichernder Stelle einerseits und Drittem andererseits unterscheiden. Ein nur innerhalb einer speichernden Stelle vorgenommener Abruf falle nicht unter die Datenschutzgesetze [20]. Graphisch stellt sich die Situation damit wie in Abb. 7.1 dar:

Abb. 7.1 "Datenabruf":



Damit würde aber dann z. B. der Sachbearbeiter, der unzulässigerweise andere als die im erlaubterweise zur Verfügung stehenden Daten zugreift, nicht wegen Datenabruf zu bestrafen sein.

19) Ringwald, INPOL und StA, § 3 I. 2. a), (S. 66).

20) Ringwald, INPOL und StA, § 3 I. 2. a), (S. 67).

Dem könnte folgende Überlegung entgegenstehen: Der Mitarbeiter einer speichernden Stelle ist nur solange nicht Dritter, wie sich seine Tätigkeit im Rahmen seines Arbeits- bzw. Anstellungsverhältnisses hält. Sobald er nicht mehr seine zugewiesene Arbeit verrichtet, sondern die ihm eingeräumte Möglichkeit nutzt, um mißbräuchlich Daten abzurufen, wird er zum Dritten. Denn er handelt jetzt beim Datenabruf nur bei Gelegenheit, nicht aber in Ausführung seiner Arbeit [21].

Auswirkungen hat dies für den Fall, in dem der Abrufende Daten aus privaten oder kommerziellen Gründen für sich selbst verwenden will, ohne daß er sie weitergibt, womit dann eine weitere etwaige Übermittlungsmodalität nicht zum Tragen kommen kann [22].

4) Die Ansicht, die einen mißbräuchlichen Abrufenden als Dritten ansieht, verhindert zum einen Strafbarkeitslücken, zum anderen führt sie zu einer Gleichstellung mit der Modalität "sich aus in Behältnissen verschlossenen Dateien verschaffen". Denn es geht weder aus den Gesetzesmaterialien, noch aus Systematik oder Sinn und Zweck der Gesetze hervor, daß der unmittelbare Zugriff auf Daten von Mitarbeitern der speichernden Stelle unterschiedlich behandelt werden soll: Ob ein Täter die Daten am Arbeitsplatz per Terminal aus einer EDV-Anlage oder "per Hand" aus einer verschlossenen Kartei entwendet, sollte an sich keinen Unterschied machen.

5) In den hier vorliegenden Verfahren wurde indessen die Problematik eines Datenabrufs innerhalb der speichernden Stelle in keinem der Fälle von den Strafverfolgungsbehörden erörtert.

21) Ringwald, INPOL und StA, in § 9 I. 1. a), (S. 67 f.), bezweifelt wohl, ob § 41 BDSG solcher Kontruktion noch zugänglich ist.

22) Zur Strafbarkeit wegen Übermittlung siehe sogleich unten, "III) Übermittlung".

II) Sich Verschaffen

Nach den meisten Datenschutzgesetzen macht sich strafbar, wer sich aus in Behältnissen verschlossenen Dateien unbefugt personenbezogene Daten verschafft [23]. Das Merkmal besteht somit aus den zwei Komponenten "sich verschaffen" und "aus in Behältnissen verschlossenen Dateien". Lediglich nach § 27 I Nr. 2 LDatG RP reicht es aus, wenn man sich die Daten "sonstwie verschafft".

1) Als "verschaffen" wird angesehen, wenn man die Daten ganz oder teilweise zur Kenntnis nimmt oder sie abschreibt, kopiert oder geistig aufnimmt [24]. Das Verschaffen beinhalte jede Art des Ansichbringen und sei als eine dem Abruf entsprechende Tathandlung anzusehen [25].

Getrennt werden müssen hier zwei unterschiedliche Begehungsweisen: Einmal die Fälle, in denen die materielle Grundlage selbst, also z. B. eine Karteikarte, mitgenommen wird, zum anderen die, bei denen lediglich Kenntnis von Daten genommen wird, die Karteikarte also abgeschrieben, kopiert oder auswendig gelernt wird. Nur im ersteren Fall sollte man von "Datendiebstahl" sprechen, während man bei den anderen Fällen von "Datenbeschaffung" reden könnte. Ausgehend davon zeigt sich, daß bei einem "Datendiebstahl" eine Bestrafung schon nach den Vorschriften des StGB möglich ist (§§ 242 ff.). Aber auch bei bestimmten Vorgehensweisen der "Datenbeschaffung" ist eine Bestrafung nach dem StGB möglich, nämlich dann,

23) § 41 I Nr. 1 BDSG und die entsprechenden Bestimmungen der Landesdatenschutzgesetze.

24) Abel/Peters Anm. 5 b zu § 25 HmbDSG; Ordemann/Schomerus § 41 Anm. 1.2.4.: Arbeitskreis Teil II S. 28/29; Hunsche in: Ruckriegel u. a., Kommentar, Erl. 5 zu § 33 LDSG NW.

25) Arbeitskreis Teil II S. 28.

wenn durch ein Aufbrechen des Behältnisses eine Sachbeschädigung begangen wird. Nötig sind die "neuen" Normen der Datenschutzgesetze dagegen nur für die übrigen Fälle der Datenbeschaffung, wie z. B. das Öffnen eines Behältnisses mit einem Nachschlüssel mit anschließendem Kopieren oder Abschreiben des Inhalts.

2) Neben der Komponente "sich verschaffen" muß noch die zweite Voraussetzung erfüllt sein: Die Daten müssen "aus in Behältnissen verschlossenen Dateien" stammen. Bei der Auslegung ist hier auf die in § 243 I Nr. 2 StGB enthaltene gleichlautende Formulierung zu verweisen [26].

3) Die Datenschutzgesetze pönalisieren also einerseits die Fälle des qualifizierten Datendiebstahls und regeln damit nochmals dasselbe wie § 243 I Nr. 2 StGB. Andererseits aber schaffen sie den Straftatbestand der "Datenbeschaffung aus verschlossenen Behältnissen". Mit dem letzteren wird das Pendant zum Datenabruf mittels technischer Mittel geschaffen: Ist beim Datenabruf ein "geistiges" Hindernis in Form entsprechender EDV-Kenntnisse bzw. programmbedinger Sicherungen zu überweinden, so liegt bei der "Datenbeschaffung" ein "körperliches" Hindernis in Gestalt eines verschlossenen Behältnisses vor.

4) Bei der Auswertung wurde zwischen "Datendiebstahl" einerseits und "Datenbeschaffung" andererseits unterschieden:

a) Nur in einem einzigen Verfahren kann man von einem "Datendiebstahl" sprechen:

26) Auernhammer, Kommentar, § 41 RN 2; Ordemann/Schomerus § 41 Anm. 1.2.4.; Grell Anm. 6 zu § 25 LDSG BW; Hunsche in: Ruckriegel u. a., Kommentar, Erl. 5 zu § 33 LDSG NW. Nach Dammann in: Simitis/D/M/R, § 41 RN 14, kann jedoch "das Schrifttum zu § 243 StGB nur bedingt herangezogen werden".

Im Fall 38 ("Karteikastenraub") [27] war gleich der ganze Karteikasten samt Karteikarten mitgenommen worden. Nach der Rechtsprechung ist § 243 I Nr. 2 StGB auch dann erfüllt, wenn der Täter das Behältnis gleich mit entwendet [28]. Wendet man diese Lösung auch auf den "Datendiebstahl" im Sinne der Datenschutzgesetze an, so wäre insoweit ebenfalls eine Bestrafung möglich.

b) Bei den Fällen einer "Datenbeschaffung" war folgendes zu beachten: In Betracht kamen einerseits die Verfahren, in denen ein Beschuldigter Einsicht in Datensammlungen genommen hatte. Andererseits war erforderlich, daß die Daten sich in verschlossenen Behältnissen befanden. Ob dies der Fall war, konnte indessen mit Hilfe der vorliegenden Aktenauswertung nicht für jedes Verfahren konkret festgestellt werden. In den Akten war nämlich dazu meist nichts vermerkt. Lediglich in drei Fällen wurde erörtert, ob ein verschlossenes Behältnis vorlag. Dabei war in zwei Verfahren für die Handlung zunächst die Modalität "abrufen" in Erwägung gezogen, dann aber abgelehnt worden, weil keine Entnahme durch technische Mittel vorgelegen habe [29].

Im dritten Verfahren (Fall 40 "Zentralnamenskartei") [30] erging gegen einen Rechtsanwalt Strafbefehl, da er sich unbefugt Daten verschafft haben soll, indem er einen anderen veranlaßte, eine Karteikarte zu fotokopieren. Nach Einspruch und

27) Der Fall wurde bereits bei § 4 C III angesprochen; eine ausführliche Darstellung findet sich im Anhang.

28) BGHSt 24, 248; weitere Nachweise bei Dreher/Tröndle, § 243 RN 25; a. A.: Schönke-Schröder-Eser § 243 RN 25.

29) Vgl. hiervon den im Anhang ausführlich dargestellten Fall 59 ("Nachbarstreitigkeiten"). Auch das vielgescholtene LG Bad Kreuznach differenzierte zwischen dem Abruf als Entnahme aus automatischen Datenverarbeitungsanlagen durch technische Mittel einerseits und dem Verschaffen andererseits; letzteres erfordere, daß der Widerstand eines Behältnisses gebrochen werde.

30) Ausführliche Falldarstellung im Anhang.

darauf folgender Hauptverhandlung wurde der Anwalt "aus tatsächlichen Gründen" freigesprochen. Zwar lag hier kein verschlossenes Behältnis vor, womit keine Bestrafung nach dem BDSG möglich gewesen wäre, das - hier anwendbare - Landesdatenschutzgesetz von Rheinland-Pfalz indessen bestraft auch den, der sich Daten "sonstwie verschafft" [31].

III) Übermittlung

Die Übermittlungsdefinition ist ein Zentralbegriff der Datenschutzgesetze [32] und gehört neben dem Dateibegriff zu den meist diskutierten Problemen. Obwohl in dieser Legaldefinition ein Verstoß gegen das Zirkularitätsverbot [33] und damit die "logische Korrektheit" [34] enthalten ist, wurde die Auswertung vorgenommen, um das Verständnis der Norm durch die Staatsanwälte zu untersuchen.

Sieht man einmal vom Verstoß gegen das Zirkularitätsverbot ab, so liegt eine "Übermittlung" wohl nur dann vor, wenn die Daten von einer speichernden Stelle (im Sinne der Definition) an einen Dritten (im Sinne der Definition) weitergegeben werden [35].

31) § 27 I Nr. 2 LDatG RP.

32) Tubies DuD 1979, 157; Kröger C. II. (S. 15). Die Übermittlung ist legaldefiniert in § 2 II Nr. 2 BDSG und in allen Landesdatenschutzgesetzen.

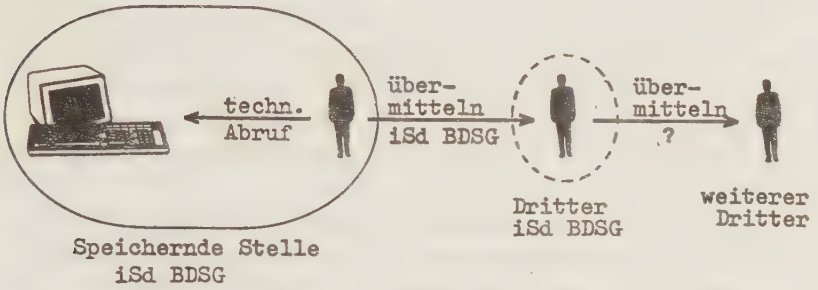
33) Siehe oben, § 3 B 3) der Arbeit.

34) Klug, Gedächtnisschrift für Rödig, S. 204.

35) Nach Schneider soll für die Frage des Geltungsbereichs des § 42 BDSG der Allgemeine Teil gelten (Gallwas/S/S RN 29 zu § 41); er will aber - entgegen systematischen und teleologischen Erwägungen der h. M. (vgl. die Nachweise bei Auernhammer, Kommentar, § 41 RN 2) - übermitteln bei § 41 nicht im Sinne der Legaldefinition, sondern "im Sinne des "Weitergebens" an andere" verstehen (RN 40, 42).

1) Ungeklärt ist, ob auch eine sich daran anschließende Weitergabe vom Übermittlungsbegriff erfaßt wird, insbesondere dann, wenn z. B. die Daten auf einem Notizzettel notiert und dieser weitergereicht wird, oder aber, wenn die Daten schlicht weitererzählt werden. Graphisch läßt sich die Situation, wie in Abb. 7.2 ausgeführt, folgendermaßen darstellen:

Abb. 7. 2 "Datenweitergabe":



Nach Ordemann/Schomerus jedenfalls ist die Weitergabe des Dritten ("Empfänger") an weitere Personen ("weitere Dritte"), d. h. der zweite Übermittlungsvorgang, nicht vom Übermittlungsbegriff erfaßt [36]:

> "Werden die Daten beim Empfänger nicht in einer Datei gespeichert, so ist eine Weitergabe durch diesen keine Übermittlung i. S. d. G. Sie werden bei ihm frei verfügbar."

36) Ordemann/Schomerus, § 2 Anm. 2.2.

Ein Dritter könnte damit straflos die Daten an einen anderen weitergeben und dieser ebenfalls straflos an wieder eine andere Person. Fraglich ist, ob der Gesetzgeber gesehen hat, daß damit einmal rechtswidrig erlangte Daten für immer straflos weitergegeben werden können, solange sie nicht wieder in Dateien gespeichert werden [37]. In der Auswertung jedenfalls wurde - unter Berufung auf Ordemann/Schomerus [38] - bei zwei Verfahren eine diesbezügliche Strafbarkeit des Beschuldigten abgelehnt, da er die erhaltenen Daten nicht in Dateien gespeichert habe u. sie so bei ihm frei verfügbar gewesen seien [39].

Das Problem stellt sich nicht, wenn man - wie Ringwald [40] - davon ausgeht, daß der ("erste") Dritte zur speichernden Stelle wird. Dann nämlich kann in der Weitergabe an den weiteren Dritten wiederum eine Übermittlung angenommen werden.

2) In der Auswertung zum Übermittlungsbegriff zeigte sich weiter, daß der Verstoß gegen das Zirkularitätsverbot nicht gesehen wurde. Bei insgesamt zehn Verfahren erfolgte eine Erörterung der Übermittlungsdefinition. Nur hier wurde gesehen, daß die Daten von der speichernden Stelle im Sinne der Datenschutzgesetze an einen Dritten im Sinne dieser Gesetze weitergegeben werden müssen.

37) Bei der Beseitigung des Verstoßes gegen das Zirkularitätsverbot sollte dies bedacht werden. Hier ist auch darauf hinzuweisen, daß bei den Vermögensdelikten die Perpetuierung einer unrechtmäßigen Lage durch § 259 StGB (Hehlerei) bestraft wird. Um so mehr sollte dies bei den persönlichkeitsbezogenen Datenschutzdelikten geschehen.

38) Ordemann/Schomerus § 2 Anm. 2.2.

39) Die Fälle 69 ("Scheidungsfolgen") und 59 ("Nachbarstreitigkeiten") werden ausführlich im Anhang vorgestellt.

40) Ringwald, INPOL und StA, § 3 V d), (S. 85).

Bei der überwiegenden Anzahl der anderen Verfahren entstand der Eindruck eines eher umgangssprachlichen Verständnisses von "übermitteln". Bei der Untersuchung nach Synonymen für eine "Datenübermittlung" stellte sich heraus, daß in beinahe zwei Drittel der Fälle das Wort "weitergeben" bzw. "Weitergabe" gebraucht wurde. Das nächst häufigste Wort ist mit knapp zwanzig Prozent "bekanntgeben".

Der Entwurf zum BDSG hatte zunächst statt "übermitteln" den Begriff "weitergeben" benutzt. Erst im Laufe der Beratungen wurde dann - wie es in der Begründung heißt - der Begriff "weitergeben" durch den "umfassenderen" Begriff "übermitteln" ersetzt [41].

Die Auswertung zeigte nun, daß die Praxis gegenteiliger Meinung ist: Das Wort "weitergeben" wird als weitergehend und umfassender angesehen, teilweise wird es sogar von den Staatsanwaltschaften, die ausführliche Erörterungen zur Legaldefinition anstellen benutzt und dem "übermitteln" vorgezogen. Dabei entstand der Eindruck, als versuche man den Begriff "übermitteln" zu meiden. Der Grund könnte darin liegen, daß "weitergeben" als eher rechtlicher und "übermitteln" als eher technischer Begriff aus der - vielen Juristen suspekten - "Computerwelt" empfunden wird [42].

Bei einer Novellierung des Gesetzes sollte deshalb beachtet werden, daß es sinnvoller sein dürfte, den Begriff "weitergeben" zu verwenden, zumal auch das BVerfG im Volkszählungsurteil fast nur den Begriff "Weitergabe" gebraucht [43].

41) BT-Drs. 7/5277 vom 2.6.1976 S. 6 ("Zu § 2").

42) Zielinski S. 129.

43) BVerfGE 65, 1 ff. = NJW 1984, 419 ff.

IV) Verändern

Nach den Legaldefinitionen ist "Verändern (Veränderung)" das inhaltliche Umgestalten gespeicherter Daten [44]. Darunter fällt nach einer ganzen Reihe von Autoren auch das Verknüpfen von Daten, jedenfalls dann, wenn dabei ein neuer Aussagewert gewonnen wird [45]. Auch wenn in der Zusammenstellung und Verknüpfung großer Datenmengen die Hauptgefahr der ADV zu sehen ist, muß diese Interpretation abgelehnt werden [46]. Sie liegt außerhalb des Wortsinns. Das inhaltliche Umgestalten von Daten ist schon sprachlich etwas anders als deren Verknüpfung [47]. Das Zusammenstellen von Daten ist schon sprachlich nicht als "verändern" anzusehen. Eine Beschränkung auf den Wortlaut jedoch ist gerade unter strafrechtlichen Gesichtspunkten geboten. Doch selbst wenn man so weit gehen sollte, daß man dem Wort "verändern" auch die Bedeutung "verknüpfen" unterlegt, ist dies höchstens datenschutzrechtlich, nicht strafrechtlich vertretbar. Denn im Strafrecht sollte die natürliche Wortbedeutung die Auslegungsgrenze sein [48]. Diese ist aber mit der Gleichsetzung von "verändern" mit "verknüpfen" überschritten, womit diese Auslegung verbotene Analogie darstellt.

44) § 2 II Nr. 3 BDSG und entsprechend die Landesdatenschutzgesetze.

45) Louis RN 193; Suppes Erl. 5 zu § 2 HDSG; Hörle/Wronka RN 13; Bergmann/Möhrle Erl. 7 zu § 2; Schmid, Polizeiblatt für BW 1980, 83.

46) Ringwald, INPOL und StA, § 3 II. 2. a), (S. 69 ff.) und § 4 II. 3. c), (S. 100 ff.); Grell Anm. 17 u. 19 zu § 4 LDSG BW.

47) Zöllner BD 1984, 242; Ringwald, INPOL und StA, § 3 II. 2. a), (S. 69 ff.); ders. JZ 1983, 283/284. Ringwald ist der Meinung, eine Datenveränderung könnte allenfalls darin gesehen werden, daß erstmals eine Abrufberechtigung eingeräumt wird, bzw. Daten eingespeichert werden (INPOL und StA, § 4 II. 3. c), (S. 100 f.); ders. JZ aaO).

48) Baumann AT § 13 I 3 (S. 154); vgl. auch die Nachweise bei FN 34 in § 3 A der Arbeit.

Fraglich bleibt indessen, ob dem Merkmal "verändern" dann noch eine eigenständige Bedeutung zukommt. Denn eine Veränderung beinhaltet notwendigerweise eine zumindest teilweise neue Speicherung und/oder Löschung [49].

Basierend auf dieser am Wortlaut als Grenze ausgehenden Interpretation wurde die praktische Relevanz dieser Modalität untersucht. Dabei stellte sich heraus, daß das Merkmal in keinem der Verfahren einschlägig war.

V) Speichern

Nach den Legaldefinitionen ist Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwekke ihrer weiteren Verwendung [50].

Die unbefugte Speicherung von Daten wird nur in den Landesdatenschutzgesetzen von Bremen und Schleswig-Holstein [51] und - folgt man der Auslegung von Kutzmann [52] - in Rheinland-Pfalz, unter Strafe gestellt. In der Strafbestimmung des BDSG ist diese Modalität nicht enthalten, da sie, wie teilweise behauptet wird, "strafrechtlich vernachlässigt werden kann" [53].

Nach den Auswertungen stellt die Speicherung in 20 Verfahren den zentralen Punkt des Vorwurfes dar, wobei es in 80 % der Fälle um Daten ging, die von Auskunfteien gesammelt worden waren. In sieben der 20 Verfahren wandte sich der Betroffene nur gegen eine Speicherung, in dreizehn primär gegen die

49) Grell Anm. 19 zu § 4 LDSG BW.

50) § 2 II Nr. 1 BDSG und die entsprechenden Bestimmungen der Landesdatenschutzgesetze.

51) § 30 I Nr. 1 BrDSG; § 23 I Nr. 1 LDSG SH.

52) Kutzmann Erl. 3 zu § 27 LDatG RP.

53) Auernhammer, Kommentar, § 41 RN 2.

Speicherung und sekundär gegen die sich daran anschließende Weitergabe ("Übermittlung") [54]. Zu diesen 20 Fällen sind indessen die - nicht gesondert erfaßten - zu zählen, in denen der Betroffene dem oder den Beschuldigten zwar expressis verbis eine Datenweitergabe vorwarf, daneben aber auch von einem stillschweigenden Vorwurf der Datenspeicherung auszugehen war.

Die Staatsanwaltschaften erörterten zwar nicht die Definition der Tatmodalität "speichern", es wurde jedoch auch in keinem der Verfahren, die alle nach § 170 II StPO eingestellt wurden, davon ausgegangen, daß eine Speicherung strafbar sei.

VI) Löschen

Nach den Definitionen ist Löschen das Unkenntlichmachen gespeicherter Daten [55] und wird nur in einigen Landesdatenschutzgesetzen als strafbare Tatmodalität angesehen [56].

Fraglich ist indessen, ob das Löschen von Daten zudem von der Vorschrift gegen Sachbeschädigung (§ 303 StGB) erfaßt wird. Angesichts der Themenstellung der Arbeit soll die Frage jedoch offen bleiben [57].

54) Vgl. oben, Abschnitt A, Tabelle 7.1 "Handlungsvarianten".

55) § 2 II Nr. 4 BDSG.

56) § 30 I Nr. 1 BrDSG; 23 I Nr. 1 LDSG SH; 21 I Nr. 1 NDSG. Nach Kutzmann (Erl. 3 zu § 27 LDatG RP) fällt unter die in § 27 I Nr. 1 gebrauchte Formulierung "sonstwie verwendet" auch das Löschen von Daten.

57) Nach Haft, DSWR 1979, 137, könnte das Löschen von Daten problemlos mit der Vorschrift gegen Sachbeschädigung (§ 303 StGB) zu erfassen sein, wenn man sich im Strafrecht zu den notwendigen Analogien bekenne.

Die praktische Relevanz der Tatmodalität "löschen" war gering. Viel häufiger war dagegen der Vorwurf, die Daten seien nicht gelöscht worden; er fällt jedoch unter die Tatmodalität "unbefugtes Speichern". Nur in einem Verfahren (Fall 41 "Tischcomputer") wurde dem Beschuldigten der Vorwurf gemacht, er habe Daten gelöscht.

Fall 41 ("Tischcomputer"):

Werbekaufmann W hatte einer wegen einer Uhr ständig am Stromnetz angeschlossenen "Tischcomputer", in dem Telefonnummern von Kunden und Geschäftspartnern sowie seine Kundentermine und verschiedene private Daten gespeichert waren. Eines Tages ließ sich das Gerät nicht mehr mit dem persönlichen Geheimcode in Betrieb nehmen, da anscheinend jemand Unbekanntes daran manipuliert hatte. W sperrte daraufhin zwei Tage die Stromzufuhr und speicherte dann alle Daten neu. Als nach drei Wochen dasselbe geschah, stellte er Strafantrag gegen Unbekannt. Die Polizei schrieb daraufhin an die Herstellerfirma und bat um technische Erläuterungen. Kurz nachdem diese eingetroffen waren und die Akte an die Staatsanwaltschaft gesandt worden war, nahm W telefonisch seinen Strafantrag zurück. Das Verfahren wurde darauf nach § 170 II StPO eingestellt, da es am Strafantrag wegen Verstoß "gegen das Datenschutzgesetz" mangle.

§ 8

Auswertung zur Strafantragsproblematik

Die Strafbestimmungen des BDSG und die fast aller Datenschutzgesetze der Länder sind reine Antragsdelikte. Lediglich in § 21 III NDSG ist vorgesehen, daß bei besonderem öffentlichen Interesse auch ein Einschreiten von Amts wegen möglich ist. Darüberhinaus kann in fünf Ländern der Datenschutzbeauftragte (bzw. die Datenschutzkommission) den Antrag stellen, in Nordrhein-Westfalen jedoch nach § 37 III 2 LDSG NW nur mit Zustimmung des Betroffenen [1].

Nach einer Einführung in die Problematik des Strafantragsrechts werden die Auswertungsergebnisse und die rechtliche Situation de lege lata dargestellt; danach erfolgt die Analyse der niedersächsischen Verfahren im Hinblick auf das Kriterium "öffentliches Interesse" [2].

A) Die Problemstellung

In den Datenschutzgesetzen wird ausgeführt "Die Tat wird nur auf Antrag verfolgt" [3]. Durch diese Formulierung allein ist aber zunächst offen, wer Antragsberechtigter ist. Lediglich in § 30 III BrDSG findet sich eine nähere Konkretisierung, da dort weiter ausgeführt wird, "neben dem Betroffenen ist auch der Landesbeauftragte für den Datenschutz antragsberechtigt." Damit ist (nur) für dieses Landesdaten-

1) § 25 III LDSG BW; § 30 III BrDSG; § 27 IV LDatG RP; § 27 III SDSG; § 33 LDSG NW.

2) Also die in § 21 III NDSG statuierte Regelung, wonach bei einer Bejahung des öffentlichen Interesses eine Strafverfolgung auch ohne Strafantrag möglich ist.

3) So § 41 III BDSG und alle Landesdatenschutzgesetze.

schutzgesetz die Frage der Antragsberechtigung gelöst. Unproblematisch ist auch das zusätzliche Strafantragsrecht der Datenschutzbeauftragten soweit es in den jeweiligen Landesgesetzen vorgesehen ist. Fraglich bleibt jedoch, wer als der "eigentlich" Strafantragsberechtigte im BDSG und in allen Landesdatenschutzgesetzen (außer Bremen) anzusehen ist. Dazu muß zunächst die im Allgemeinen Teil des StGB statuierte Vorschrift des § 77 StGB herangezogen werden, wonach "der Verletzte" den Antrag stellen kann. Für die Bestimmung des "Verletzten" wird somit wieder auf das entsprechende Gesetz, hier also die Datenschutzgesetze, zurückverwiesen. Während nun die stillschweigende Verweisung von den Datenschutzgesetzen auf § 77 StGB noch klar und nachvollziehbar ist, bleibt der zur Auslegung des Begriffs "Verletzter" notwendige Rückverweis auf die Datenschutzgesetze problematisch: Soll als Verletzter der "Betroffene" (im Sinne der Datenschutzgesetze) gelten, oder aber die Stellen, die die Daten speichern? Besonders beim sog. "Datendiebstahl" ist umstritten, inwieweit ein Strafantragsrecht der "speichernden Stelle" besteht [4].

Vor der Darstellung der Behandlung dieses Problems durch die Staatsanwaltschaften soll untersucht werden, wer in den 159 Verfahren die Strafanträge gestellt hat (Frage der Person der Antragstellung).

4) Der Begriff "speichernde Stelle" ist § 2 III Nr. 1 BDSG legaldefiniert (ebenso in allen Landesdatenschutzgesetzen) Zum Strafantragsrecht der speichernden Stelle ausführlich sogleich weiter unten im Abschnitt C. Zur Abgrenzung "Datendiebstahl" und "Datenbeschaffung" als Varianten des "sich aus in Behältnissen verschlossenen Datei verschaffen", siehe oben, § 7 B II der Arbeit.

B) Auswertung der tatsächlichen Strafantragsteller

Die Auswertung konzentrierte sich auf die Frage, wer tatsächlich den Strafantrag gestellt hat. Dabei wurde es als jeweils ein Strafantrag angesehen, wenn ein Betroffener (im Sinne der Datenschutzgesetze) [5], ein Landesdatenschutzbeauftragter oder aber eine speichernde Stelle einen Antrag stellte. Strafanträge anderer als der Genannten wurden nicht gewertet. Waren mehrere Betroffene in einem Verfahren vorhanden, so wurde auch bei mehrfacher Antragstellung nur ein Strafantrag registriert. Als Strafantrag wurden auch die neun später zurückgezogenen, sowie die sieben verspätet gestellten Anträge gewertet. Unter dem Begriff "speichernde Stelle" wurden auch die Stellen erfaßt, die Daten im Auftrag verarbeiten, also die "weite" Auslegungsvariante zugrundegelegt [6].

Das Ergebnis der Auswertung ergibt sich aus Tabelle 8.1 "Strafantragsteller":

Tabelle 8.1 "Strafantragsteller":	
Antrag eines Betroffenen:	110 mal
Antrag speichernde Stelle:	16 mal
Antrag Landesbeauftragter:	0 mal

5) In § 2 I BDSG ist die Definition des "Betroffenen" in der Legaldefinition der "personenbezogenen Daten" enthalten: "Im Sinne dieses Gesetzes sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)."

6) Dazu ausführlich sogleich im Abschnitt C.

I) Strafanträge von Landesdatenschutzbeauftragten

Überraschend ist zunächst, daß in keinem einzigen Fall Strafantrag von einem Landesbeauftragten für den Datenschutz (LfD) gestellt wurde. Allerdings ereigneten sich von den 26 Fällen, die ausweislich der Akten auch ihnen bekannt sein mußten, nur die Hälfte in Ländern mit Strafantragsrecht der Datenschutzbeauftragten. Da sich zudem ein Antragsrecht nur bei Verstössen ergibt, die im Anwendungsbereich des jeweiligen Landesgesetzes liegen, blieben so nur noch fünf Verfahren übrig; in keinem indessen wurde Strafantrag gestellt. Die Berechnung der fünf Verfahren ergibt sich aus Tabelle 8.2 "Strafantragsmöglichkeit LfD":

Tabelle 8.2 "Strafantragsmöglichkeit LfD":

Alle einem LfD bekannten Fälle		26
Bundesgesetz einschlägig	-	10
Landesgesetz ohne Antragsrecht	-	2
Unaufklärbar/keine Datei	-	9
Landesgesetz mit Antragsrecht	=	5

II) Strafanträge von Betroffenen

Eine weitere Untersuchung befaßte sich mit den Anträgen von Betroffenen. Sie ergab, daß in 21 der 159 Verfahren ein Betroffener deshalb gar keinen Antrag stellen konnte, da er von der Staatsanwaltschaft überhaupt nicht informiert worden war. Bedenklicherweise waren in knapp neunzig Prozent der Fälle jeweils mehr als zehn Betroffene zu verzeichnen.

Problematischer ist jedoch, daß in acht der 21 Verfahren gerade der fehlende Strafantrag des Betroffenen als Einstellungsgrund diente:

Fall 42 ("HEPOLIS [7]-Abruf"):

Ein junger Polizeibeamter versuchte über Funk von ca. zwei Dutzend Personen, deren Namen und Geburtsdatum er angab, in Erfahrung zu bringen, ob und wenn ja warum diese im HEPOLIS gespeichert sind. Der am Terminal sitzende Beamte wurde jedoch mißtrauisch, da alle Personen ungefähr das gleiche Alter hatten und die Namen alphabetisch aufgeführt waren. Er verweigerte daraufhin die Auskunft.

Diesen Sachverhalt bekam der Staatsanwalt von der Polizei mitgeteilt. Daraufhin stellte er wenige Tage später das Verfahren ein, "da die erforderlichen Strafanträge nicht gestellt" seien. Jedoch fand sich in der ganzen Akte keinerlei Hinweis darauf, daß der Staatsanwalt irgendwelche Ermittlungen angestellt und versucht hatte, die (namentlich bekannten) Betroffenen zu befragen, ob sie Strafantrag stellen wollten oder nicht.

Genau dieselbe Vorgehensweise und Einstellungsbegründung findet sich bei den sieben anderen Verfahren, wie z. B. in den beiden folgenden Fällen:

Fall 43 ("Studentenkartei"):

Assistenzarzt A wurde von einem anonymen Anrufer bei der Polizei beschuldigt, Adressen von Erstsemestern an die Verbindung V geliefert und damit gegen "das Datenschutzgesetz" verstoßen zu haben. Auf telefonische Befragung durch die Polizei erklärte der Leiter der Verwaltung, daß es am (medizinischen) Fachbereich der Universität eine Studentenkartei gäbe, die aber nur dem Büropersonal und dem Prüfungsausschuß zugänglich sei. Ärzten oder anderen Personen würde daraus keine Antwort gegeben. Dieser Sachverhalt wurde der Staatsanwaltschaft mitgeteilt, die das Verfahren sogleich nach § 170 II StPO einstellte: "Es handelt sich um ein Antragsdelikt. Geschädigte haben keinen Strafantrag gestellt."

7) HEPOLIS = Hessisches Polizeiinformationssystem. Zu den polizeilichen Informationssystemen ausführlich: Ringwald, StA und INPOL, § 1 (S. 23 ff.).

Fall 44 ("Interessenverein"):

Der Angestellte eines Rechenzentrums leitete über 1 000 Adressen geschiedener Frauen und Männer an einen "Geschiedenen-Interessenverein" weiter, damit dieser Werbeschreiben versenden konnte. Dieser Sachverhalt wurde von einem Vorstandsmitglied des Vereins (der selbst nicht betroffen war) mitgeteilt.
Ohne weitere Ermittlungen wurde das Verfahren mit der Begründung, es fehle ein Strafantrag, eingestellt.

Möglicherweise jedoch haben sich in all diesen acht Fällen die Staatsanwälte an Nr. 6 II RiStBV [8] gehalten. Danach müssen sie die "Strafverfolgung im öffentlichen Interesse für geboten halten", damit es "angebracht sein kann" (so jeweils wörtlich Nr. 6 II RiStBV) den Antragsberechtigten zu unterrichten und anzufragen, ob ein Strafantrag gestellt wird. Wenn die Staatsanwaltschaft aber in diesen Fällen schon das öffentliche Interesse verneint haben, dann wäre zumindest ein entsprechender Aktenvermerk (wie dies in drei Fällen geschah) bzw. eine andere Einstellungsbegründung nötig gewesen.

Bei den 21 Verfahren, in denen die Betroffenen keinerlei Kenntnis von ihrem Strafantragsrecht hatten, wäre dennoch in acht Verfahren eine Strafverfolgung möglich gewesen. Voraussetzung wäre allerdings, daß man der "speichernden Stelle" ein Antragsrecht zubilligt [9]. Sie hatte nämlich hier in diesen acht (sowie acht weiteren) Verfahren "Strafantrag" gestellt. Es ist deshalb zu prüfen, ob ein Strafantragsrecht der speichernden Stelle besteht und wie die Staatsanwaltschaften das Problem lösten.

8) Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV). Abgedruckt als Anhang H 1 bei Kleinknecht, StPO.

9) Dazu sogleich § 8 C II der Arbeit.

C) Strafantragsrecht der "speichernden Stelle"?

Einer ausführlichen und gesonderten Erörterung bedürfen die 16 Fälle, in denen die speichernde Stelle (auch "Herr der Daten" genannt [10]) einen Strafantrag stellte, denn es ist umstritten, ob ihr dieses Recht überhaupt zusteht [11]. Wie oben dargelegt [12], wurde der Begriff "speichernde Stelle" in seiner weitesten Auslegung verwandt, um möglichst viele Fälle hierunter erfassen zu können. Allerdings waren in den 16 Verfahren nur zweimal Service-Rechenzentren beteiligt, die ja nur von einem Teil der Kommentatoren unter § 2 III Nr. 1 BDSG subsumiert werden [13]. Bei allen anderen Fällen lag nach allen Meinungsgruppen eine "speichernde Stelle" im Sinne des § 2 III Nr. 1 BDSG vor.

I) Die Ergebnisse der Auswertung

Die Behandlung der Strafantragsproblematik durch die Staatsanwaltschaften war unterschiedlich. Es lassen sich drei Fallgruppen bilden:

1) In zwei, bereits vorgestellten, Verfahren beschäftigten sich, wie aus entsprechenden Vermerken hervorging, die Staatsanwälte mit dem Problem und lehnten ein Strafantragsrecht der speichernden Stelle ab:

10) So Hergenhahn DuD 1977, 27; Ruckriegel, Kommentar Anm. 10 zu § 2 LDSG NW. Nach Ringwald, StA und INPOL, § 2 II. 4. (S. 54) ist der Begriff "irreführend, assoziert er doch ähnliches wie Eigentum an Informationen".

11) Bejahend: Bergmann/Möhrle, Anm. 8 zu § 41; Schneider in: Gallwas/S/S § 41 RN 61; Ordemann/Schomerus Anm. 4 zu § 41; von Uckermann DuD 1978, 67. Verneinend: Auernhammer, Kommentar § 41 RN 10; Dammann in: Simitis/D/M/R § 41 RN 33; Grell Anm. 12 zu § 25 LDSG BW; Kamlah in: Burhenne/Perband § 41 RN 19; Sendler DuD 1977, 62; Tegtmeyer ÖVD 1981, S. 14.

12) Siehe oben Abschnitt B.

13) So fallen nach Auernhammer, Kommentar § 2 RN 15; Schweinoch in: Gallwas § 8 RN 7, 23; Rissing-van Saan S. 173/174; Ordemann/Schomerus § 2 Anm. 3.2; Marx DSWR 1979, 87 f. Service-Rechenzentren unter den Begriff "speichernde Stelle"; a. A.: Dammann in: Simitis/D/M/R § 2 RN 148; Louis RN 42; Schimmel in: Burhenne/Perband § 2 RN 102. Vgl. zum Ganzen auch Ringwald, StA und INPOL, § 3 III. 1. a) (S. 72 f.).

- Im Fall 21 ("Mikrofichesfund") [14] wurde daraufhin ein Betroffener angeschrieben, der dann Strafantrag stellte.

- Im Fall 24 ("Mitgliederabwerbung") [15] verneinte die Staatsanwaltschaft erst nach einem entsprechenden Hinweis des Rechtsanwaltes des Beschuldigten das Antragsrecht der speichernden Stelle. Sie stellte daraufhin das Verfahren mangels Strafantrages ein, obwohl keiner der namentlich bekannten Betroffenen gefragt worden war.

2) In zwei weiteren Verfahren [16] erörterte die Polizei, ob der "Herr der Daten" [17] (nur hier tauchte dieser Begriff ausdrücklich auf) ein Strafantragsrecht habe. Die Staatsanwaltschaft ging darauf nicht ein. Der Grund könnte sein, daß beidesmal mangels Tatverdacht nach § 170 II StPO eingestellt wurde.

3) In 12 Verfahren wurde die Strafantragstellung durch die "speichernde Stelle" von der Staatsanwaltschaft stillschweigend akzeptiert. Für die Beschuldigten wirkte sich dies in den drei Verfahren aus, die nicht mit einer Einstellung nach § 170 II StPO endeten. Es handelt sich zum einen um die schon vorgestellten Fälle 1 ("Universitätsoperator") [18] und 25 ("Mikroficheeinsicht") [19], die beidesmal für den Beschuldigten mit einem Strafbefehl endeten. Zum anderen ist im bereits kurz angeschnittenen Fall 26 ("Zeitungsabonnenten") [20] der Beschuldigte wegen § 41 BDSG verurteilt worden, obwohl nur der Strafantrag des Service-Rechenzentrums und nicht eines Betroffenen vorlag.

14) Bereits vorgestellt bei § 5 A V 3) b). Ausführliche Falldarstellung im Anhang.

15) Bereits vorgestellt, § 5 A V 3) b). Ausf. Falldarstellung im Anhang.

16) Fall 15 ("Nachbarsjunge") und Fall 45 ("Löschungsbegehren"). Fall 45 sogleich, unten Abschnitt C; ausf. Falldarstellung im Anhang.

17) Vgl. dazu FN 10.

18) Vorgestellt oben, § 3 B IV. Ausführliche Falldarstellung im Anhang.

19) Vorgestellt oben, § 5 A V 3)b). Ausführliche Falldarstellung im Anhang.

20) Vorgestellt oben, § 5 A V 4). Ausführliche Falldarstellung im Anhang.

In den Akten des Falls 26 fand sich zur Frage des Strafantrages nur die Formulierung "Vorsorglich stelle ich Strafantrag für alle Fälle", die der Geschäftsführer des Rechenzentrums als Abschlußsatz in der polizeilichen Vernehmung verwandte. Da sich das Gericht im Verhandlungsprotokoll dann auf diesen "Strafantrag des Rechenzentrums" bezog, wurde dieser Antrag der speichernden Stelle anscheinend auch für § 41 BDSG als ausreichend angesehen. Nimmt man noch die Formulierungen der Urteilsbegründung dazu, nach der die Daten nur mit Zustimmung der Eigentümer weitergegeben hätten werden dürfen, so läßt dies darauf schließen, daß das Gericht (personenbezogenen) Daten Eigentumsqualität zugemessen hat. Das Strafantragsrecht wäre dann jedoch, wie bei § 248a StGB, Ausfluß der materiellen Rechtsgüter "Eigentum" und "Gewahrsam".

II) Die Auslegung des Strafantragsrechts

Fraglich ist indessen, ob neben den Betroffenen auch die speichernde Stelle ein Antragsrecht hat: Dies wäre dann der Fall, wenn die vom Begriff "Verletzten" in § 77 StGB ausgehende Rückverweisung auf die Datenschutzgesetze sowohl den Betroffenen, als auch die speichernde Stelle erfaßt.

1) Eine Reihe von Autoren scheint dies anzunehmen, denn sie gibt dem "Herrn der Daten" (wie die speichernde Stelle auch genannt wird) ein Antragsrecht für den Fall, in dem ein sog. "Datendiebstahl" (§ 41 I Nr. 2 "... oder sich aus in Behältnissen verschlossen Dateien verschafft ...") vorliegt [21].

21) Bergmann/Möhrle, Anm. 8 zu § 41; Schneider in: Gallwas/S/S § 41 RN 61; Ordemann/Schomerus § 41 Anm. 4.; von Uckermann DuD 1978, 67; Arzt, die Ahndung von Verstößen, S. 136, spricht sich in diesem Fall einerseits dafür aus, daß das Strafantragsrecht des Betroffenen dann auszuschliessen sei, andererseits bezeichnet er dies dann als "zweifelhaft". Den Ausführungen ist indessen nicht zu entnehmen, daß die Autoren zwischen "Datendiebstahl" und "Datenbeschaffung" differenzieren (dazu oben, § 7 B II der Arbeit).

Die speichernde Stelle sei neben dem Betroffenen als Verletzter im Sinne von § 77 I StGB und damit als Antragsberechtigter im Sinne der datenschutzrechtlichen Strafnormen anzusehen. Als Begründung wird angeführt, der speichernden Stelle "gehöre" die Datei. Dies bedeutet wohl, daß man Daten Vermögenswert zumißt und sie deshalb wie Eigentum behandelt.

2) Diese Ansicht, die speichernde Stelle sei Verletzter und somit beim "Datendiebstahl" antragsberechtigt, stellt indessen eine falsch verstandene Rückverweisung dar und ist somit abzulehnen [22]. Sie entbehrt jeder praktischen Notwendigkeit, läßt sich nicht mit Sinn und Zweck der Datenschutzgesetze vereinbaren und verwischt die Grenze zur Computerkriminalität.

Schon aus der Formulierung "Datendiebstahl" wird deutlich, daß anscheinend nur bei dieser Fallgruppe ein Strafantragsrecht bestehen soll. Bei einer "Datenbeschaffung", also der bloßen Kenntnisnahme vom Inhalt ohne gleichzeitige Wegnahme eines Datenträgers, soll damit wohl kein Antragsrecht bestehen [23]. Der "Datendiebstahl" jedoch, der nur eine besondere Form des schweren Diebstahls nach 243 I Nr. 2 StGB darstellt, ist schon über § 243 StGB hinreichend pönalisiert. Somit werden die Strafnormen der Datenschutzgesetze insoweit überflüssig. Zudem sollte man Daten nicht leichtfertig wie Eigentum behandeln [24]. Informationen können zwar Vermögenswert haben,

22) Ebenfalls gegen ein Strafantragsrecht: Auernhammer, Kommentar § 41 RN 10; Dammann in: Simitis/D/M/R § 41 RN 33; Grell Anm. 12 zu § 25 LDSG BW; Kamlah in: Burhenne/Perband § 41 RN 19; Sendler DuD 1977, 62; Tegtmeyer ÖVD 1981, 14.

23) Zur "Datenbeschaffung" siehe oben, § 7 B II der Arbeit.

24) Steinmüller, Der Schutz "medizinischer" Daten, S. 136. Grundsätzlich zum Problem "Eigentum an personenbezogenen Daten": Meister, Datenschutz, S. 101 ff.

sind aber dem Wesen nach grundverschieden, was schon aus dem Volkszählungsurteil des BVerfG [25] folgt. Denn dort wurde das "informationelle Selbstbestimmungsrecht" des Einzelnen über seine Daten nicht aus Art. 14 GG, sondern aus dem in Art. 2 I GG iVm Art. 1 I GG geschützten allgemeinen Persönlichkeitsrecht abgeleitet. Sinn des § 41 BDSG kann es somit nur sein, über § 243 StGB hinaus eine Bestrafung zu ermöglichen. Dem Betroffenen sollte bei Diebstahl seiner Daten die Möglichkeit gegeben werden, eine Strafverfolgung zu erzwingen, nicht aber sollte dem Eigentümer und dem Gewahrsamsinhaber eine zweite Strafnorm zur Verfügung gestellt werden [26]. Sinnvoll wäre § 41 als zweite Strafnorm neben § 243 StGB nur, wenn man ihr insoweit eine "Sperrwirkung" gegenüber § 243 StGB einräumt, als bei Vorliegen eines Datendiebstahls eine Verfolgung nur nach Strafantrag der speichernden Stelle (nach § 41 BDSG) möglich wäre. Diese Interpretation findet aber weder im Wortlaut, noch in den Gesetzesmaterialien, noch im Sinn und Zweck des Gesetzes eine Stütze. Sie wäre zudem eine vom Gesetzgeber wohl nicht gewollte Einschränkung des für § 243 StGB geltenden Offizialprinzips. Somit ist für die Fälle des Datendiebstahls ein Strafantragsrecht der speichernden Stelle aus § 41 BDSG abzulehnen [27]. Die vom Begriff "Verletzter" des § 77 StGB ausgehende Rückverweisung auf die Datenschutzgesetze erfaßt damit lediglich den Betroffenen; nur er hat ein Strafantragsrecht, nicht aber die speichernde Stelle. Dies gilt ebenfalls für die Fälle der

25) BVerfGE 65, 1 ff. = NJW 1984, 419 ff.

26) Das gleiche läßt sich auch für den Fall ausführen, daß der Täter nur das Behältnis beschädigt und Daten abschreibt, womit keine Wegnahme im Sinne des Diebstahls vorliegt. Der Besitzer des Behältnisses hat dann die Möglichkeit, Strafantrag wegen Sachbeschädigung (§ 303 StGB) zu stellen, "benötigt" also auch hier keine zweite Strafnorm. Wegen § 45 BDSG verdrängt § 303 StGB die Norm des § 41 BDSG (Gola/Hümmerich/Kerstan, S. 14). Dem Betroffenen dagegen, dessen Daten abgeschrieben wurden, bleibt nur die Strafnorm des entsprechenden Datenschutzgesetze.

27) Auernhammer, Kommentar, § 41 RN 10; Dammann in: Simitis/D/M/R § 41 RN 33; Grell Anm. 12 zu § 25 LDSG BW; Kamlah in: Burhenne/Perband § 41 RN 19; Sendler DuD 1977, 62 und Tegtmeyer ÖVD 1981, 14.

"bloßen Datenbeschaffung" [28]. Denn auch hier ist nicht die speichernde Stelle verletzt, sondern der Betroffene.

3) Zusammenfassend ist damit festzuhalten, daß de lege lata bei richtig verstandener Rückverweisung auch bei der Modalität "sich aus in Behältnissen verschlossenen Dateien verschaffen" nach § 41 I Nr. 2 BDSG kein Strafantragsrecht der speichernden Stelle besteht.

D) Öffentliches Interesse bei § 21 III NDSG

Da nach § 21 III NDSG eine Strafverfolgung auch bei Vorliegen eines öffentlichen Interesses möglich ist, wurden die 18 niedersächsischen Verfahren daraufhin untersucht, wie sie in dieser Frage von den Staatsanwaltschaften behandelt wurden.

Bei der Hälfte dieser Verfahren war objektiv gesehen nur das BDSG anwendbar. Die Staatsanwaltschaft prüfte indessen in einem Verfahren "§ 41 BDSG in Verb. mit § 21 NDSG" und verneinte ein öffentliches Interesse [29]. Bei der anderen Hälfte der Verfahren kamen die Strafverfolgungsbehörden in 7 Fällen gar nicht zu der Frage, ob ein öffentliches Interesse an der Strafverfolgung bestehe, da nach ihrer Auffassung schon kein hinreichender Tatverdacht vorlag. In den beiden restlichen Verfahren wurde die Frage des öffentlichen Interesses einmal erörtert und einmal nicht:

28) Dazu oben, § 7 B II der Arbeit.

29) Fall 68 ("Handwerkersorgen"); ausführliche Falldarstellung im Anhang.

Im Fall 45 ("Löschungsbegehren") [30]

rief ein Polizeibeamter die Daten seines Vaters (auf dessen Wunsch) über Terminal ab, da er überprüfen wollte, ob und welche Speicherung vorlag. Die Staatsanwaltschaft stellte das Verfahren ein, da der Vater keine Strafantrag gestellt habe und ein öffentliches Interesse an der Strafverfolgung nicht bestehe.

Im Fall 46 ("Meisteranerkennung") [31]

waren von einer Handwerkerinnung Daten weitergegeben worden. Nach Beschwerde des Betroffenen stellte der Generalstaatsanwalt das Verfahren ein, da die Strafantragsfrist verstrichen gewesen sei.
Er übersah wohl die Möglichkeit eines Einschreitens aufgrund eines öffentlichen Interesses [32].

30) Ausführliche Falldarstellung im Anhang.

31) Ausführliche Falldarstellung im Anhang.

32) Übersehen wurde wohl auch, daß die Daten nie in einer Datei, sondern immer nur in Akten gespeichert waren.

§ 9

Zusammenfassende Würdigung und Reformvorschläge

Im Schlußkapitel der Arbeit sollen nach einer Zusammenfassung und Würdigung der Ergebnisse (Abschnitt A) zunächst kurz Reformüberlegungen allgemein-datenschutzrechtlicher Natur gemacht werden. Darauf aufbauend werden datenschutzstrafrechtliche Novellierungsgedanken entwickelt und die Arbeit mit dem konkreten Vorschlag einer Strafnorm abgeschlossen (Abschnitt B).

A) Zusammenfassende Würdigung

Faßt man die Ergebnisse der Normanalyse und der Auswertungen zusammen,so kann man die komplizierte Verweisungstechnik [1] der Datenschutzgesetze als "Stolperstein" für die Strafverfolgungsbehörden qualifizieren. Unter normtheoretischer Betrachtungsweise offenbart sich das gesamte Gesetz wegen der komplizierten Verweisungstechnik, insbesondere den Subsidiaritätsregelungen, als höchst problematisch. Es ist mit dem rechtsstaatlichen Gebot der Normenklarheit und strafrechtlichen Bestimmtheit kaum vereinbar und deshalb verfassungsrechtlich äußerst bedenklich [2]. Die strukturelle und quantitative Komplexität der Strafnorm [3] führt in der Praxis zu Fehleinschätzungen, insbesondere des Regelungsumfangs der Gesetze. Die häufigsten Fehler betrafen die Anwendungsvoraussetzungen [4].

1) Dazu ausführlich § 3 der Arbeit; dort wird in der Abb. 3.3 "Verweisungsbaum" (§ 3 B I) und in Abb. 3.4 "Sprachliche Auflösung" (§ 3 B III) plastisch die Komplexität gezeigt.

2) Siehe dazu oben, § 3 B der Arbeit.

3) Vgl. dazu die Graphik (Abb. 3.2 "Komplexitätsfolgen"), oben § 3 A III der Arbeit.

4) Damit befaßt sich § 5 der Arbeit.

So wurde z. B. einerseits das Erfordernis einer Datei verkannt, andererseits nicht gesehen, daß im öffentlichen Bereich zwischen zwei Datenschutzgesetzen differenziert werden muß [5]. Die meisten Fehler entstanden, weil die Staatsanwälte vom bloßen Wortlaut der Strafnorm ausgingen und somit die sich erst aus den impliziten Verweisungen erschließenden Einschränkungen und Modifizierungen übersahen.

Doch nicht nur die Gesetze als Ganzes, sondern auch die einzelnen Tatmodalitäten der datenschutzrechtlichen Strafbestimmungen unterliegen Bedenken:

Das Tatbestandsmerkmal "übermitteln" verstößt gegen das Zirkularitätsverbot und ist deshalb verfassungsrechtlich äußerst problematisch [6].

Die Modalität "abrufen" erfaßt nur den Datenabruf durch technische Mittel [7].

Das Merkmal "verändern" ist durch die vom Wortlaut der Legaldefinition gebotenen einschränkenden Auslegung strafrechtsempirisch überflüssig [8].

Die Modalität des "sich aus in Behältnissen verschlossenen Dateien verschaffen" ist von geringer praktischer Relevanz, da die meisten Fallkonstellationen bereits vom StGB (§§ 242 ff., § 303) erfaßt werden.

5) Dazu insbesondere § 5 A IV der Arbeit.

6) Siehe § 3 B II 3) der Arbeit.

7) Siehe § 7 B I der Arbeit.

8) Siehe § 7 B IV der Arbeit.

9) Siehe § 7 B II der Arbeit.

Daneben zeigte sich, daß die Strafverfolgungsbehörden die Tatmodalitäten zumeist umgangssprachlich verstehen; sie gehen vom bloßen Wortlaut aus und übersehen die Verweisungen auf die Legaldefinitionen [10].

I) Tatsächliches Ausmaß der Delikte und Dunkelziffer

Diese gravierenden Mängel der Datenschutzgesetze scheinen ihre praktische Relevanz zu verlieren, angesichts der geringen Zahl von nicht einmal 200 Ermittlungsverfahren in 5 Jahren, von denen zudem beinahe 80 % durch Einstellung nach § 170 II StPO endeten [11]. Es entsteht zunächst der Eindruck, als seien Datenschutzdelikte ein vernachlässigbares Randproblem der Gesamtkriminalität. Doch dieser Anschein trügt, abgesehen von den Schwierigkeiten generalpräventative Effekte [12] zu messen [13]. Die Dunkelziffer dürfte schon jetzt - ähnlich wie bei der Computerkriminalität - beträchtlich hoch sein. Nicht jeder Täter verhält sich so "dumm" wie jener Polizeibeamte im Fall 42 ("HEPOLIS-Abruf") [14], der gleich Daten über zwei Dutzend alphabetisch geordnete Personen auf einmal abfragen wollte: Hätte er sie über ein paar Tage verteilt oder direkt über ein Terminal ohne dazwischengeschaltete Funkleitzentrale abgefragt - die Tat wäre sicher nie aufgedeckt worden.

Die Höhe der Dunkelziffer indessen läßt sich schwer schätzen, wenn auch die folgende Überlegung das mögliche Ausmaß zu ver-

10) Nach Schneider, NJW 1984, 392, enthalten die Datenschutzgesetze "eine Reihe von Legaldefinitionen, die formal und praxisfremd sind".

11) Siehe die Statistik in der Tabelle 4.5 "Verfahrensbeendigung", oben § 4 C IV.

12) "der Zweck der Strafgesetze ist der, daß der Fall seiner Anwendung gar nicht vorkommt" Fichte, Grundlagen des Naturrechts nach den Principien der Wissenschaftslehre. Zweiter Teil oder Angewandtes Naturrecht, Jena/Leipzig 1797, § 20 (zitiert nach: Gesamtausgabe, Werkeband I/4, Stuttgart-Bad Cannstatt 1970, 60).

13) Heinz, wistra 1983, 134.

14) Fall 42 ("HEPOLIS-Abruf"), § 8 II 2) der Arbeit.

deutlichen vermag: Zur Zeit werden allein von der SCHUFA täglich ca. 90 000 Auskünfte erteilt [15]. Unterstellt man, daß von 10 000 Auskünften nur eine einzige mißbräuchlich ist, so kommt man allein hier auf über 3 000 Auskunftserschleichungen im Jahr. Dazu kommen aus dem privaten Bereich noch die Fälle, in denen (andere) Auskunfteien [16] über das Vorliegen eines berechtigten Interesses im Sinne von § 32 II BDSG getäuscht werden, sowie all die Fälle, in denen Mitarbeiter von Unternehmen auf die von diesen genützten EDV-Anlagen zugreifen. Die gleichen Überlegungen gelten für den öffentlichen Bereich, in dem vor allem die besonders schwer zu überführenden Alleintäter agieren [17]. Hier braucht man nur an die Mitte 1982 bereits installierten 2 500 Terminals zu denken, die an das System INPOL [18] des BKA angeschlossen sind [19], das über 7 Mio. Datensätze enthalten soll und auf das fast jeder Polizeibeamte über Funk (zumindest teilweise) zugreifen kann [20]. Welche Dynamik allein die Möglichkeit eines Zugriffes entwickelt, zeigt sich z. B. daran, daß sich die Anfragen an das vom Kraftfahrbundesamt betriebene

15) Vgl. oben § 5 A IV.

16) Nach Mallmann AWD 1973, 84 erteilten allein die Vereine Creditreform 5 Mio. Auskünfte im Jahr 1972. Vgl. auch oben, § 5 A IV FN 33.

17) Die beschuldigtenbezogene Auswertung ergab, daß im öffentlichen Bereich (Behörden und sonstige öffentl. Stellen) die Zahl der Alleintäter überdurchschnittlich hoch ist.

18) Elektronisches Informtions- und Auskunftssystem für die Polizei. Dazu ausführlich und umfassend: Ringwald, INPOL und StA, § 1 (S. 23 ff.).

19) Küster, Das System INPOL, S. 62; nach Steinmüller, DVD-Jahrestagung 1978, S. 45, werden es im Endausbau 14 000 Terminals sein. Vgl. dazu auch Ringwald, INPOL und StA, § 1 (S. 23 ff.).

20) So Kubica, Kriminalistik 7/8-1981 S. 317, für das Jahr 1983. Nach Küster, Das System INPOL, S. 66, kann über den Kriminalaktennachweis (KAN) auf Akten von 2 Mio. Personen zugegriffen werden. Ringwald, INPOL und StA, § 1 I. 2. c), (S. 28), legt dar, daß am 1.1.1982 im zentralen Personenindex ca. 2,15 Mio. Personen nachgewiesen waren.

System ZEVIS [21] von Januar 1982 bis September 1982 von 50 000 auf über 100 000 pro Monat verdoppelt haben [22]. Unterstellt man auch hier jede zehntausendste Abfrage als mißbräuchlich, so zeigt dies erneut die hohe Dunkelziffer.

II) Gründe für eine hohe Dunkelziffer

Neben den "allgemeinen" Ursachen, die zu einer Dunkelziffer führen [23], dürfte der maßgebliche Grund für eine hohe Dunkelziffer bei den Datenschutzdelikten darin liegen, daß der "Faktor Mensch" ausgeschaltet ist: Ein Computer wird nicht mißtrauisch. Wohl kann man gewisse Plausibilitätsroutinen einbauen, aber auch sie lassen sich umgehen. Selbst die bei vielen Systemen bestehenden umfangreichen Protokollierungspflichten sind wertlos, solange der Täter nicht durch sein Verhalten Anlaß zur Kontrolle gibt. Will man beispielsweise im öffentlichen Bereich über ein fingiertes Amtshilfeersuchen Daten erhalten, so dauert dies lange und bringt wenig an Informationen, nämlich nur die bei der "ersuchten" Behörde gespeicherten Daten. Zudem besteht das Risiko, daß der um Hilfe ersuchte Kollege Verdacht schöpft. Auch beim heute oft gebräuchlichen,mehr informellen Gebrauch des Telefons ist der Informationsfluß gering. Schon um keinen Verdacht beim anderen aufkommen zu lassen, wird man sich bei den fingierten Fällen mit den "notwendigen" Informationen begnügen. Mit Einführung von Terminals und Anschluß an verschiedene Datenbanken ändert sich die Situation grundlegend: Nun kann man nicht nur schneller, sondern auch umfassender

21) Zentrales Verkehrsinformationssystem; dazu Ringwald, INPOL und StA, § 1 I. 11. (S. 36).

22) Julich, Informationsverbund Ordnungsbehörden - Polizei, S. 159.

23) Ausführlich dazu Göppinger, Kriminologie, S. 159 ff., der aber den Begriff "Dunkelfeld" geeigneter hält (S. 159).

Informationen erhalten, denn in EDV-Systemen sind in der Regel mehr Daten über den Einzelnen enthalten als in den herkömmlichen Systemen [24]. Um ein Persönlichkeitsbild zu erhalten, sind nun nicht mehr eine Vielzahl von (schriftlichen oder telefonischen) Anfragen an verschiedene "ersuchte" Personen zu richten, die dann begründet werden müssen, sondern nur verschiedene "codes" einzutippen. Es ist einfacher per Knopfdruck die gespeicherten Daten zu erhalten, als wenn jeweils jemand gebeten werden muß, in Akten oder anderen Schriftstükken nachzusehen. Zudem dürfte es psychologisch weniger hemmend sein, eine Maschine zu "täuschen", als einen Menschen, d. h. es ist weniger kriminelle Energie nötig [25]- bei größerem Schaden. Diese Überlegungen gelten nicht nur bei Amtshilfeersuchen, sondern auch bei den Fällen der sog. Auskunftserschleichung. Besonders dann, wenn direkt über ein Terminal Auskunft eingeholt werden kann, ist die Gefahrt groß, daß das berechtigte Interesse über die willkürliche Eingabe eines anerkannten Grundes vorgetäuscht wird. Selbst wenn alle Abfragen protokolliert würden, fände keine Überprüfung statt, da kein Mensch eingeschaltet ist, der mißtrauisch werden könnte. Da zudem die Zahl der Abfragen generell in dem Maß steigen werden, wie sie einfacher werden, wird bei dieser steigenden Anzahl der Abfragen auch kein Vorgesetzter mehr in der Lage sein, eine Überprüfung im notwendigen Umfang vorzunehmen [26].

Es wurde somit gezeigt, daß durch die Ausschaltung des "Faktor Mensch" in den Datenübermittlungsvorgängen die Gefahr des Mißbrauchs gestiegen ist und als maßgeblicher Grund für eine hohe Dunkelziffer angesehen werden muß.

24) So auch Simon/Taeger, Rasterfahndung, S. 69.

25) So auch Göppinger, Kriminologie, S. 672.

26) Überflüssig ist damit die Protokollierung nicht, denn ohne sie - und dies zeigte sich besonders bei Auskunfteien - ist eine Aufklärung und Strafverfolgung fast unmöglich.

III) Zukünftige Entwicklung

Die Zahl der installierten Anlagen und die der Terminals hat erst in den letzten Jahren eine weitere Verbreitung gefunden und teilweise ist die Aufstellung erst im Gange. Somit steigen schon objektiv die Mißbrauchsmöglichkeiten [27]. Ferner muß berücksichtigt werden, daß die Strafvorschriften der Datenschutzgesetze,wie bei jedem neuen Gesetz, erst ins Bewußtsein der damit befaßten Stellen kommen müssen und somit in den ersten Jahren noch verhältnismäßig wenig Delikte angezeigt wurden. Für die Zukunft ist hier eine Veränderung zu erwarten [28]. Besonders dann, wenn die jetzt verschobene Volkszählung stattgefunden hat, werden die Anzeigen steigen, denn bei Verdacht (der durch die Zählung sensibilisiert werden wird) der unbefugten Speicherung oder Weitergabe von Daten wird dies als Verstoß gegen "das Datenschutzgesetz" angesehen und angezeigt werden. Schließlich wird durch die mit der Einführung der sog. "Neuen Medien" verbundene Diskussion [29] eine erhöhte Datenschutz-Sensibilität zu erwarten sein.

Aus all diesen Gründen heraus wird somit in Zukunft einerseits die Datenschutz-Kriminalität zunehmen und andererseits werden die Strafanzeigen wegen Verstoßes gegen "das Datenschutzgesetz" steigen [30].

27) So auch Stadler DuD 1981, 5 und wohl auch Bull DuD 1982 S. 147 und Simon/Taeger, Rasterfahndung, S. 69.

28) Bereits die Kriminalstatistik des Jahres 1983 bestätigt die Prognose eindrucksvoll: Die Verstöße gegen das Bundes- (Landes-) Datenschutzgesetz haben um neunzig Prozent zugenommen, d. h. sie haben sich fast verdoppelt.

29) Vgl. nur die verschiedenen Beiträge in NJW 1984 Heft 8. Schneider, NJW 1984, 393, spricht inzwischen von einer "Sensibilisierung breiter Bevölkerungsschichten".

30) Haefner, S. 181, rechnet mit einer Zunahme der "Informationskriminalität". Die Kriminalstatistik für das Jahr 1983 mit ihrer neunzigprozentigen Zunahme der Datenschutzdelikte ist ein erstes Indiz dafür.

IV) Schlußfolgerungen

Es fragt sich, wie die Entwicklung mit Hilfe des Strafrechts aufgehalten werden kann [31]. Mit den gegenwärtigen Strafnormen jedenfalls ist dies nicht zu bewältigen. Sie erweisen sich bei näherer Betrachtung als lückenhaft.

1) So sind zum einen personenbezogene Daten, die nicht zur Übermittlung bestimmt sind und in nicht-automatisierten Verfahren verarbeitet werden ("interne Daten") vom Schutzbereich der Strafnormen ausgenommen. Auch die vom "Medienprivileg" erfaßten Daten genießen keinen strafrechtlichen Schutz [32].

2) Desweiteren wird der Anwendungsbereich des § 41 BDSG aufgrund der Subsidiaritätsregel des § 45 BDSG immer stärker eingeengt, denn jedes neue bereichsspezifische Gesetz wirkt sich auf den Regelungsumfang aus. Solange diese neugeschaffenen Bereichsvorschriften keine eigene Strafnorm enthalten und auch nicht auf § 41 BDSG verweisen, schwindet jedesmal ein Stück des Schutzbereichs des § 41 BDSG [33]. Denn, wenn die personenbezogenen Daten nicht mehr "von diesem Gesetze" [34], d. h. dem BDSG, sondern von einem bereichsspezifischen Gesetz geschützt werden, ist auch kein strafbewerter Verstoß dagegen möglich. Schon heute bestehen solche Datenschutzgesetze (im weiteren Sinne), die eine Strafbarkeit nach § 41 BDSG ausschließen. Es sei nur an den Kata-

31) Nach Ansicht von Lenckner, Tübinger FS S. 252, dürfte die allgemeine Entwicklung vor allem dazu führen: "Zu einem verstärkten Einsatz des Strafrechts gegen Gefahren, die uns von der modernen Technik drohen."

32) Vgl. dazu oben, § 5 B der Arbeit.

33) So enthält z. B. das Melderechtsrahmengesetz (MRRG) vom 16.8.1980 (BGBl. I S. 1429) keine eigene Strafnorm und keinen Verweis auf das BDSG, während § 79 SGB X (vom 16.8.1980, BGBl. I S. 1469) auf § 41 BDSG verweist.

34) Nach § 41 BDSG wird bestraft, wer "von diesem Gesetz geschützte personenbezogene Daten unbefugt ...". Wie Dammann in NJW 1978, 1906 f. ausführt, verkannte dies auch das LG Bad Kreuznach (NJW 1978, 1931 f.).

log des § 45 BDSG erinnert [35]. Wird gegen Vorschriften dieser Gesetze verstoßen, so ist keine Bestrafung nach § 41 BDSG möglich. Da zudem in den wenigsten dieser bereichsspezifischen Datenschutzgesetzen eigene Strafvorschriften normiert sind [36], öffenen sich hier weite Strafbarkeitslücken.

Diese, zu Straflücken führende Eigenschaft von bereichsspezifischen Datenschutzgesetzen gilt auch im Bereich der Ländergesetzgebung. Die Landesdatenschutzgesetze schützen nämlich ebenfalls nur die vom jeweiligen Landesgesetz erfaßten Daten [37].

Zu bedenken ist indessen, daß mit dem Erlaß von bereichsspezifischen Gesetzen zugleich die Herausnahme dieser Daten aus dem Schutzbereich der Datenschutzgesetze vom Gesetzgeber gewollt sein kann; nur dann liegt aber eine bewußte und keine verweisungsbedingte Strafbarkeitslücke vor.

3) Zu diesen, die Datenschutzgesetze in ihrer Gesamtheit betreffenden, Einschränkungen kommen noch die Begrenzungen durch einzelne Tatmodalitäten:

Bewertet man der Verstoß gegen das Zirkularitätsverbot als verfassungswidrig, so ist keine Strafbarkeit der "Datenweitergabe" gegeben [38].

Das Merkmal "abrufen" erfaßt nicht, wie es der Wortlaut suggeriert, jeden Datenabruf, sondern nur einen technischen Abruf zwischen speichernder Stelle und Drittem [39].

37) Nach Laufer/Steinbrinck, S. 272, gibt es Schätzungen, wonach ca. 600 Spezialbestimmungen dem BDSG vorgehen. Vgl. auch das bei Kutzmann, Einführung, S. 8 - 13, aufgestellte tabellarische Verzeichnis.

36) Vgl. nur das soeben in FN 33 erwähnte MRRG.

37) Auch alle Landesdatenschutzgesetze bestrafen nur die "von diesem Gesetz geschützten Daten".

38) Gerade im Strafrecht spricht m. E. viel dafür, daß auch formale Verstöße die Verfassungswidrigkeit begründen. Zum Verstoß gegen das Zirkularitätsverbot siehe oben, § 3 B II 3).

39) Siehe § 7 B I der Arbeit.

Zu bemängeln ist schließlich, daß die Tatmodalität "speichern" sowohl im BDSG, als auch in den meisten Landesdatenschutzgesetzen fehlt [40].

4) Neben diesen Strafbarkeitslücken sind auf der anderen Seite überflüssige Regelungen vorhanden:

Das in den Strafnormen statuierte Tatbestandsmerkmal "verändern" kann nicht im Sinne von "verknüpfen" interpretiert werden, da "verknüpfen" kein "inhaltliches Umgestalten" darstellt [41]. Da in den 159 Verfahren - auch bei großzügigster Interpretation - in keinem einzigen Fall ein "inhaltliches Umgestalten" zu erkennen war [42], ist dies ein Indiz für die praktische Bedeutungslosigkeit dieser Tatmodalität.

Die Tathandlung "sich aus in Behältnissen verschlossenen Dateien verschaffen" schließlich ist insoweit überflüssig, als die meisten Handlungsvarianten bereits vom Kernstrafrecht (§§ 243 ff., § 303) erfaßt werden [43].

40) Dazu § 7 B V. Für eine Strafbewehrung dieser Tatmodalität sind: Garstka DuD 1982, 156; Leuze/Schedler/Schneider ÖVD 10/1980 S. 12; Schneider in: Gallwas/S/S § 41 RN 2; Schweinoch/Geiger Einl. zum BayDSG S. 23; Louis RN 351; Rissing-van Saan S. 269 und wohl auch Simon/Taeger, JZ 1982, 141, da sie sogar schon die Erhebung von Daten einbeziehen wollen. Die Mehrheit der Datenschutzkommission des Deutschen Juristentages schließlich wollte den Schutz schon an die Sammlung personenbezogener Daten anknüpfen (S. 24). Dagegen: Auernhammer, Kommentar, § 41 RN 2, da das Speichern strafrechtlich vernachlässigt werden könne.

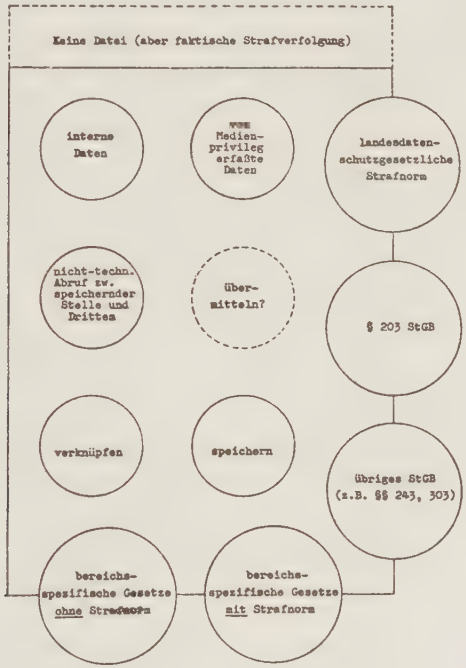
41) Nach den Legaldefinitionen (z. B. § 2 II Nr. 3 BDSG) ist Verändern "das inhaltliche Umgestalten gespeicherter Daten".

42) Dazu oben, § 7 B IV der Arbeit.

43) Dazu oben, § 7 B II der Arbeit.

5) Notwendig sind somit Korrekturen an diesen "verweisungsgeschädigten" Strafnormen des Bundes- und der Länderdatenschutzgesetze. Wie sehr z.B. die Geltung des § 41 BDSG eingeschränkt ist und wie grundlegend die Änderung sein muß, mag die Abb. 9.1. veranschaulichen:

Abb. 9.1. "§ 41 BDSG -Strafbarkeit":



Bevor jedoch ein konkreter Vorschlag gemacht werden kann, ist zu klären, von welchen Prinzipien sich diese Strafnormänderung leiten lassen muß. Es sollen deshalb zunächst Überlegungen "allgemein-datenschutzrechtlicher Natur" angestellt werden, um zusätzliche Entscheidungshilfen für die Ausgestaltung zu bekommen.

V) Die Datenschutzprinzipien "Einwilligung" und "Zweckbindung"

Zunächst sind die den Datenschutzgesetzen zugrundeliegenden Prinzipien der Einwilligung und Zweckbindung daraufhin zu untersuchen, ob sie geeignet und zweckmässig sind, die Datenschutzkriminalität zu verhindern oder zumindest zu erschweren[44].

1)Kein allein entscheidendes Kriterium kann die Frage der Einwilligung sein. Dieses Kriterium versagt bei offenkundigen Daten ganz und auch bei den anderen Daten ist es nur eingeschränkt tauglich: Wer die vorformulierten Einverständniserklärungen zur Datenweitergabe in den (weitgehend identischen) Banken-AGBs ("SCHUFA-Klausel")[45] nicht akzeptiert, kann kein Konto eröffnen und keinen Kredit aufnehmen[46]. Wer bei der straßenverkehrsrechtlichen Zulassung seines Autos nicht, wie in den Formularen gefordert, seinen Beruf angibt, müßte versuchen seine Zulassung erst gerichtlich zu erzwingen - und gibt dann lieber den Beruf an. Die Liste der Beispielsfälle ließe sich beliebig fortsetzen. Gemeinsam ist allen, daß die Verweigerung der Einwilligung nur theoretisch möglich ist, faktisch aber durch wirtschaftlichen oder psychologischen Druck erzwungen wird[47]. Die Problematik entspricht strukturell der der Allgemeinen Geschäftsbedingungen[48]. Der Unterschied besteht darin, daß es ein AGB-Gesetz gibt, das z.B. bestimmte Klauseln verbietet und andere nur eingeschränkt erlaubt. Die Datenschutzgesetze sind in dieser

44) Die Sensitivität von Daten kann nach dem Volkszählungsurteil des BVerfG (E 65, 1 ff.) nicht mehr als (entscheidendes) Kriterium für die Gefährlichkeit der EDV angesehen werden.

45) Zu den (neuen) SCHUFA-Klauseln: Großmann DSWR 1980, 278 ff.

46) So auch die Bedenken von Louis RN 166.

47) Simitis VersR 1981, 203; Louis RN 70 u. 166; Leuze/Schedler/Schneider ÖVD 10/1980 S. 15; Simon DANA 1/1982 S. 18; zum psychologischen Zwang vgl. auch Ringwald NJW 1982, 2594.

48) Ebenso Egloff/Schimmel, DuR 1977, S. 136.

Beziehung unzureichend. Sie regeln nur unvollkommen, wer welche Daten erheben oder nicht erheben darf. Für die Zukunft bleibt allerdings die Hoffnung einer "Ausstrahlungskraft" des Volkszählungsurteils [49]. Wirkungen zeigt das vom Bundesverfassungsgericht postulierte "informationelle Selbstbestimmungsrecht" jedenfalls schon insoweit, als es zu einer "Verunsicherung der Verwaltungsapparate" geführt hat [50].

2) Als weiteres Prinzip des Datenschutzes ist das der Zweckbindung zu nennen [51]. Das Bundesverfassungsgericht führt dazu aus: "Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. ...Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt [52]." Damit gilt die Zweckbindung nicht nur für die Weitergabe, sondern auch für die Erhebung von Daten. Es wurde also erkannt, daß durch eifriges Sammeln von Informationen eine Datenübermittlung überflüssig werden kann. Denn wer alle Daten, die er irgendwann (und für welchen Zweck auch immer) zu benötigen glaubt, selbst sammelt, ist nur beschränkt auf Datenaustausch angewiesen [53]. In den letzen Jahren wurden die Datenbestände in den Behörden (und Personalinformationssystemen der Unternehmen) erstaunlich intensiv ausgebaut. Man hat den Eindruck, daß nach dem Scheitern des Personenkennzeichen und damit eines einfachereren Datenaustausches, als Alternative das eigene Sammeln von Daten gewählt wurde.

49) BVerfGE 65, 1 ff. = NJW 1984, 419 ff.

50) So Stuttgarts Polizeipräsident Dr. Vermander in: computer magazin 6/1984 S. 6.

51) Simitis VersR 1981, 204 "Grundprinzip allen Datenschutzes ist die strikte Zweckbindung".

52) BVerfG NJW 1984, 422.

53) Vgl. Gallwas, Der Staat 1979, S. 513.

Dabei entwickelten nicht nur die Behörden [54] (aber diese besonders), sondern auch die Unternehmen einen ausgeprägten "Datenhunger" [55]. Durch das Urteil des Bundesverfassungsgerichts wird nun zumindest den Behörden und sonstigen öffentlichen Stellen diese Ausweichmöglichkeit genommen. Denn "die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken" ist mit dem Recht auf informationelle Selbstbestimmung nicht zu vereinbaren [56]. Deshalb ist es zu begrüßen, daß einige Landesgesetzgeber bereits früher schon einen in diesem Zusammenhang richtigen Ansatzpunkt gewählt haben, indem sie das unbefugte Speichern von Daten unter Strafe gestellt haben [57].

3) Zusammenfassend läßt sich feststellen:

Das Prinzip "Einwilligung" ist wenig geeignet vor den Gefahren moderner EDV-Anlagen zu schützen, während das Prinzip der Zweckbindung eine wichtige und unverzichtbare Funktion im Rahmen der Datenschutzgesetze erfüllt [58].

54) Vgl. dazu Herden/Karrer VOP 1981, 365.

55) So wörtlich Becker Schleswig-Holsteinische Anzeigen 1980 S. 25; vgl. auch Hase, DuR 1984, 44, der von einem "enormen Datenhunger der Behörden" spricht.

56) BVerfG NJW 1984, 423. Bestritten ist allerdings, ob dies auch für die private Wirtschaft gilt; dafür: Simitis NJW 1984, 399; dagegen: Krause JuS 1984, 268 FN 4; vgl. auch Geiger DSWR 1984, 46.

57) § 30 I Nr. 1 BrDSG; § 23 I Nr. 1 LDSG SH und nach der Kommentierung von Kutzmann (Erl. 3) auch § 27 LDatG RP. Für eine Strafbarkeit der unbefugten Speicherung sind auch die oben in FN 35 angeführten Autoren.

58) Zur Problematik der Bindung der Daten an den jeweiligen Zweck - an die Aufgabe, vgl. aber Ringwald, INPOL und StA, S. 103 ff. (S. 111 ff.). Nach Ringwald ist dann auch zu bestimmen, nach welchen Kriterien Aufgaben von anderen Aufgaben abgegrenzt werden können.

VI) Das "Quantitätskriterium" als tragendes Prinzip des Datenschutzes

Entscheidendes Kriterium für computerspezifischen Mißbrauch sollte die Menge darstellen, d.h. die Fülle der Informationen ("Quantitätskriterium"). Die Gefahr des "gläsernen Menschen", d.h. für jeden durchschaubar zu sein, wächst mit jeder zusätzlichen Information, sei sie nun sensitiv, fast neutral oder gar offenkundig. Die Gefahr liegt in der mosaikartigen Zusammenstellung einzelner Daten zu einem "Persönlichkeitsbild" [59]. Bereits heute gibt es Personalinformationssysteme in denen über jeden Arbeitnehmer bis zu 400 Daten gespeichert sind [60]; zu gerichtlichen Auseinandersetzungen führten schon Systeme, die bis zu 10.000 Arbeitnehmerdaten miteinander verknüpfen können [61]. Viele dieser Systeme beinhalten die Möglichkeit eines Profilabgleichs [62] und im Bundesverteidigungsministerium werden bereits Beförderungen mit Hilfe von Personalinformationssystemen durchgeführt [63].

Der Grund für diese Systeme liegt neben allgemeinen Rationalisierungsgesichtspunkten darin, daß einerseits die Unternehmen bestrebt sind, Mitarbeiter möglichst rationell einzusetzen und

59) Rissing-van Saan S. 3; Haft BT, § 11 I 2.; ders. NJW 1979, 1197; ders. DSWR 1979, 141.

60) Kilian, Personalinformationssysteme, S. 2; nach Cobler, S. 14, sind es zwischen 50 und 1 000 Daten.

61) Vgl. den Streit um das System Paisy bei OPEL von dem LAG Frankfurt: DANA 5/1983 S. 13. Vgl. auch Meister, Datenschutz, S. 18, der von Systemen mit 11 000 Zeichen (bytes) pro Mitarbeiter spricht. Nach Heller, DVR-Tagung 1982, S. 49, sind bereits 1 000 Daten nicht akzeptabel und es sei durchaus möglich, mit unter 200 auszukommen.

62) Schon 1977 gab es Personalinformationssysteme, die die Möglichkeit des "Profilabgleichs" enthielten: Kilian JZ 1977, 485. Über ein Drittel der Systeme enthalten Fähigkeitsprofile der Arbeitnehmer: Kilian, Personalinformationssysteme, S. 117.

63) So Bull DANA 1/1981 S. 6.

dafür entsprechende Daten benötigen. Andererseits besteht ein immer stärker wachsender Bedarf des Staates an Daten [64]. So zwingen schon heute 126 Gesetze und Verordnungen ein Unternehmen, insgesamt 214 Daten über einen Mitarbeiter zu speichern [65]. Diese Beispiele zeugen sowohl von einem "Datenhunger" der staatlichen wie auch der privaten Stellen. Je mehr Daten aber über den Einzelnen gespeichert sind, desto mehr besteht die, vom BVerfG schon in der Mikrozensus-Entscheidung [66] gesehenen, Gefahr, daß der Mensch in seiner ganzen Persönlichkeit registriert und katalogisiert und damit wie eine Sache behandelt wird, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist. Ein wirksamer Datenschutz darf deshalb nicht beim Aufstellen von Kriterien wie dem Vorliegen einer Datei, dem Erfordernis einer Einwilligung oder der Orientierung am Verwendungszweck stehenbleiben, sondern muß eine Kontrolle der Datenmenge, die ja das Wesen der Datenverarbeitung ausmacht [67], vorsehen und auch (wie vom BVerfG gesehen) die Datenerhebung einbeziehen [68].

In der Einleitung fast aller Kommentare zu den Datenschutzgesetzen wird darauf abgestellt, Wesensmerkmal der EDV sei die Fähigkeit, riesige Datenmengen schnell und zuverlässig miteinander zu verbinden. Eine Steigerung der Informationsverarbeitungskapazitäten gekoppelt mit einer hohen und zeitlich

64) Hase, DuR 1984, 44, spricht von einem "enormen Datenhunger der Behörden".

65) So die Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) vom 30.4.1984; abgedruckt in "computer zeitung" vom 16.5.1984, S. 26. Ähnlich bereits früher Hentschel bei Herb DSWR 1981, 253.

66) BVerfGE 27, 1, 6.

67) Bull, 2. TB des BfD (= BT-Drs. 8/3570) S. 71; Ernesti NJW 1983, 512; vgl. auch Ringwald, INPOL und StA, S. 92 ff.

68) So auch Geiger DSWR 1984, 46 und Simon/Taeger JZ 1982, 142: "Unberechtigte Datenerhebung wird durch das informationelle Selbstbestimmungsrecht ausgeschlossen".

fast unbegrenzten Speicherbarkeit stelle das Kennzeichen der Computer dar [69]. Weiter wird ausgeführt, daß damit Persönlichkeitsbilder geschaffen und die Bürger transparent gemacht werden könnten. Die "gebändigte Quantität drohe in ungebändigte Qualität umzuschlagen" [70]. All diese Argumente werden dafür verwandt, die generelle Notwendigkeit von Datenschutzgesetzen verständlich zu machen. Führt man sie jedoch konsequent zu Ende, so muß die Menge der verarbeiteten Daten zum zentralen Maßstab eines Schutzes vor den Gefahren der EDV gemacht werden [71]. Auch die Ausführungen des Bundesverfassungsgerichts sind in dieser Richtung zu verstehen, denn das Gericht betonte besonders die Gefahr von Persönlichkeitsbildern, die um so genauer sind, je mehr Daten vorlägen [72]. Somit wurde konkludent das Quantitätskriterium angesprochen, denn die Registrierung und Katalogisierung des einzelnen verlangt ja gerade eine Vielzahl von Daten.

Zusammenfassend läßt sich somit das Quantitätskriterium als tragendes Prinzip des Datenschutzes bezeichnen.

69) Auernhammer, Kommentar, Einf. RN 11; Berg JA 1984, 245; Bull, 2. TB des BfD (= BT-Drs. 8/3570) S. 71; Ernesti NJW 1983, 512; Grell, Einf. LDSG BW, Anm. 5; Ordemann/Schomerus, Einl. Anm. 1; Simitis in: Simitis/D/M/R, Einl. RN 12; Schweinoch/Geiger, Einl. BayDSG Erl. 1; Woertge S. 27.

70) Grell, Einf. Anm. 7; ähnlich Kafer S. 510 und Hempfer VBlBW 1982, 188; nach Benda, FS Geiger S. 37, wird durch die Möglichkeit Persönlichkeitsprofile anzulegen die Gefahr verstärkt, daß der Staat den Menschen in seiner ganzen Persönlichkeit registriert und katalogisiert.

71) So auch Schünemann ZStW 90 (1978) S. 24 FN 36.

72) BVerfG NJW 1984, 419, 421.

VII) Konsequenzen des Quantitätskriteriums

Als sinnvolle Ergänzung der gegenwärtigen Konzeption des Datenschutzes ist deshalb die Berücksichtigung des Quantitätskriteriums erforderlich. Nur so kann man die auch vom Bundesverfassungsgericht gesehene Gefahr von Persönlichkeitsbildern abwenden [73]. Die Diskussion um die Frage, ob zwei, drei oder vier Merkmale für das Vorhandensein einer Datei vorliegen müssen [74], ist geeignet den Eindruck zu erwecken, als sei diese Anzahl EDV-spezifisch. Gerade aber das Gegenteil ist der Fall. Es sind eher Erörterungen darüber anzustellen, ob es eine Anzahl ("Menge") von Daten gibt, ab der grundsätzlich eine Beeinträchtigung der Persönlichkeit vorliegt und wenn ja, wie hoch diese Menge ist. Diese Überlegung verdeutlicht auch, daß der oft kritisierte Adressenhandel solange nicht eine Gefahr für die Persönlichkeit des Einzelnen darstellt, als er sich innerhalb der Bestimmungen des § 24 II BDSG bewegt. Zwar mag es für Einzelne unangenehm oder lästig sein, bestimmte Warensendungen zu erhalten [75], eine Gefährdung seines persönlichen Bereichs durch EDV-Anlagen ist darin aber nicht zu erkennen.

Nicht die einzelnen Mißbrauchsfälle stellen eine Gefahr dar, sondern das mit EDV-Anlagen errichtete System der Mißbrauchsmöglichkeiten. Nicht das Persönlichkeitsrecht eines einzelnen, das aller steht auf dem Spiel [76]. Bei der Schaffung rechtlicher Regelungen ist deshalb zu berücksichtigen, daß mit dem Aufbau eines EDV-Verbundes gleichzeitig ein latentes Mißbrauchssystem erzeugt wird. Die gewichtigste Erkenntnis der Untersuchung

73) BVerfG NJW 1984, 419, 421.

74) Vgl. dazu § 5 A I der Arbeit.

75) Vgl. dazu den im Anhang dargestellten Fall 33("Reklamesendung").

76) So wörtlich Ringwald, INPOL und StA, § 4 II. 3. (S. 100).

zur Datenschutzkriminalität ist deshalb: Nicht so sehr die einzelen betrachtete Auskunftserschleichung gefährdet den persönlichen Bereich des Einzelnen, sondern vielmehr die Errichtung elektronischer Auskunftssysteme an sich, sei es nun durch Auskunfteien oder staatliche Stellen.

Die EDV, das sei hier betont, ist ein notwendiges und unverzichtbares Werkzeug für Produktion, Verwaltung und Kommunikation. "Maschinenstürmertendenzen" und Horrormeldungen sind ebensowenig angebracht wie kritiklose Fortschrittsgläubigkeit und Computer-Euphorie. Notwendig ist die Bewertung des Computers als Werkzeug wie jedes andere auch. Es läßt sich nicht nur gebrauchen, sondern auch mißbrauchen. Dabei stehen den enormen Nutzen und Fähigkeiten einer EDV-Anlage spiegelbildlich außerordentliche Gefahren gegenüber. Computer werden einen Siegeszug antreten wie weiland das Automobil und sie werden wie jenes mißbraucht und zweckentfremdet werden. Da indessen die Gefahren ungleich höher sind, müssen auch die rechtlichen und technischen Schutzvorkehrungen um so sorgfältiger und umfassender errichtet werden [77].

Die bestehenden Datenschutzgesetze jedenfalls und erst recht deren Strafbestimmungen dürfen hierbei nur als ein erster Schritt betrachtet werden. Sie sind in ihrer heutigen Konzeption nicht in der Lage, einen ausreichenden Schutz für den Einzelnen zu gewährleisten, da sie nicht an die Eigenheiten und Wesensmerkmale von Computern anknüpfen, die darin bestehen, große Mengen von Daten schnell und sicher zusammenzuführen. Gerade aber die Quantität stellt, wie oben ausgeführt [78], den entscheidenden Faktor dar, so daß Lösungen rechtlicher (und technischer) Art mit Hilfe des Quantitätskriteriums gefunden werden müssen. Dies gilt es bei der Novellierung der Datenschutzgesetze und insbesondere deren Sanktionsnormen zu bedenken.

77) Nicht umsonst wurde der Begriff "Datenverkehrsordnung" gebraucht: Schomerus ZRP 1981, 291 ff. und Weise DuD 1983. 69 f.

78) § 9 A VI der Arbeit.

B) Datenschutzrechtliche Reformvorschläge

Aufbauend auf die obigen Überlegungen sollen deshalb zunächst einige kurze Vorschläge gemacht werden, die zur Abwehr computerspezifischer Gefahren geeignet sind und als flankierende Maßnahmen strafrechtliche Sanktionsnormen unterstützen helfen.

Betont werden muß als erstes, daß die rechtlichen Sicherungen entscheidend sind. Dies sei am Beispiel des neuen computerlesbaren Personalausweises [79] gezeigt:

Die Kritiker des neuen Ausweises wollen ihn verhindern, da er in den "Überwachungsstaat à la Orwell's Big Brother" führe [80]. Doch selbst wenn dies so wäre, die Vereitelung seiner Einführung wäre nur ein Scheinsieg: In Kürze werden Computer auch die normalen, herkömmlichen Ausweise lesen können [81]. Eine Überwachung wäre dann aber rein technisch gesehen auch ohne den neuen Ausweis möglich. Dies verdeutlicht, daß nicht die technische Ausprägung eines Ausweises entscheidend ist, sondern vielmehr die rechtlichen Gegebenheiten. Nur durch rechtliche Absicherungen läßt sich ein "Überwachungsstaat" verhindern, nicht aber durch Boykott oder Vernichtung von Ausweisen und ähnlichen Aktionen [82]. Notwendig ist ein funktionierender Rechtsstaat mit den entsprechenden Gesetzen,"dessen Stärke nicht darauf beruht, daß er allwissend" ist [83].

79) Die bereits schon einmal auf den 1.1.1984 verschobene Einführung der Ausweise wurde infolge des Volkszählungsurteils des BVerfG (E 65, 1 ff.) erneut verschoben (computer magazin 6/1984 S. 6).

80) Vgl. dazu Bölsche, Der Wege in den Überwachungsstaat, Reinbek bei Hamburg 1979.

81) Das Schriftlese-System SLS von Siemens kann sogar schon handgeschriebene Blockschrift lesen: "computer zeitung" vom 21.3.1984, S. 66; zur Möglichkeit Photographien zu erkennen vgl. oben, § 6 FN 34.

82) Vgl. nur den in DANA 6/1983 S. 46 ff. abgedruckten "Fahrplan für eine Kampagne gegen Personalkarte und Erfassungsstaat".

83) Hirsch DANA 5/1982 S. 4.

I) Allgemeine Reformüberlegungen

Die zweckmäßigste rechtliche Lösung zur Abwehr der aus der Computertechnologie entstehenden Gefahren besteht in der Kontrolle und Normierung der Systeme. So könnte man, wie heute bei PKWs, zu einer Zulassungspflicht von Hardware und konsequenterweise auch Software kommen [84]. Dies hätte für die Hardware- und Softwareproduzenten gleichzeitig den Vorteil eines erhöhten Schutzes vor Mißbrauch. Besonders für die immer mehr in ihrer Bedeutung steigende Software könnte die Zulassungspflicht den "Softwarediebstahl" bzw. die unberechtigte Anfertigung von Kopien ("Raubkopien") drastisch einschränken [85]: Wenn nur noch zugelassene Software verwendet werden darf, werden sich für nicht zugelassene (weil entwendete und abgewandelte) Programme nur wenig Käufer finden, die solche rechtswidrigen Programme zu verwenden bereit sind. Und beim Antrag auf Zulassung angeblich selbst entwickelter, in Wahrheit aber kopierter und veränderter Programme, würden diese dann als "Raubkopien" erkannt werden.

Auch für den Schutz des einzelnen, des Betroffenen, bringt dieses Verfahren Vorteile: Die Zulassung könnte an die Verwirklichung systembedinger Sicherungen vor Mißbrauch gebunden werden, womit schon bei der Konzeption der Software der Schutz des Einzelnen berücksichtigt werden müßte. Eine Zulassungspflicht könnte so z.B. verhindern, daß Programme auf den Markt

84) In ähnlicher Weise äußert sich Sieglerschmidt (DuD 1981, 238) in Entsprechung einer Entschließung des Europäischen Parlamentes vom Mai 1979 (siehe DuD 1981 S. 235 u. S. 238 FN 37). Vgl. auch Herb NJW 1983, 2238 und DSWR 1984, 27. Die Datenschutzkommission des Deutschen Juristentages (S. 17/18) schlug schon 1974 eine "präventive Kontrolle durch das Erfordernis des Genehmigungsverfahrens" vor. Zur Programmbetriebskontrolle vgl. auch Steinmüller DVR 1983, 300 FN 354.

85) Vgl. dazu den im Anhang dargestellten Fall 67 ("Programmdoppelung").

kommen, die ein Übermaß an personenbezogenen Daten("Quantitätskriterium") enthalten. Auch die Möglichkeit von Profilabgleichen oder Persönlichkeitsbilder könnte kontrolliert und eingeschränkt werden.

Eine weitere Absicherung könnte man dadurch erreichen, daß alle datenverarbeitenden Stellen verpflichtet werden, dem Betroffenen einen jährlichen "Kontoauszug" über die zu seiner Person gespeicherten Daten zu senden [86]. Zweckmäßigerweise sollte auch hier das Quantitätskriterium berücksichtigt werden, indem z.B. die Mitteilungspflicht erst entsteht, wenn eine bestimmte Anzahl von Daten pro Person überschritten wird.

II) Strafrechtliche Reformüberlegungen

Die obigen Ausführungen haben die Notwendigkeit einer modifizierten Konzeption des Datenschutzes deutlich gemacht. Bei den als nötig festgestellten Änderungen datenschutzrechtlicher Strafnormen ist die Orientierung am "Quantitätskriterium" geboten [87]. Zu prüfen ist jedoch zuvor, ob überhaupt eine Strafnorm nötig ist.

Der Schutz der Persönlichkeits- bzw. Privatsphäre des Einzelnen wird de lege lata nicht nur über die bestehenden Strafnormen der Datenschutzgesetze zu sichern versucht, sondern ist auch in einer Reihe von Vorschriften, wie z.B. § 203 StGB, geregelt. Somit ist von einer grundsätzlichen gesetzgeberischen Überzeugung des Erfordernisses strafrechtlicher Absicherung

86) So Haefner, S. 181, und auch die Überlegungen eines Arbeitskreises der Deutschen Vereinigung für Datenschutz e. v. (DVD) in: DANA 5/1979 S. 17. Für den Bereich der Personalinformationssysteme: Rumpf DSWR 1982, 131.

87) Siehe § 9 A VI der Arbeit.

auszugehen. Auch in der Literatur wird gefordert, "den Informationsmißbrauch rechtlich stärker negativ zu bewerten"[88]. Bei der Auswertung zeigte sich, daß das Vorhandensein einer Strafnorm "des Datenschutzgesetzes" als selbstverständlich vorausgesetzt wird. Die Akzeptanz der Norm in der Bevölkerung ist gewährleistet.

Die grundsätzliche Notwendigkeit einer Strafnorm ergibt sich ferner auch daraus, daß anscheinend nur so eine Durchsetzung der Vorschriften über die Datenverarbeitung möglich ist [89]. Nach Auswertung der Ermittlungsverfahren (besonders denen mit Beteiligung von Handelsauskunfteien) drängt sich der Verdacht auf, daß nur die Existenz von Sanktionsnormen die Einhaltung der datenschutzrechtlichen Vorschriften gewährleistet. Auf Grund des sich vielfach in den Akten vorhandenen Schriftwechsels zwischen Aufsichtsbehörde und Beschuldigten entstand der Eindruck, daß der Behörde die Durchsetzung ihrer Vorstellung von einer ordnungsgemäßen Datenverarbeitung nur mit Hilfe der Drohung mit dem Staatsanwalt gelang [90]. Auch den Betroffenen war es oft nur möglich, über die Staatsanwaltschaft zu erfahren, wer der Auskunftsuchende war und was er als berechtigtes Interesse vorgeschoben hatte,um somit eine unbefugte Datenübermittlung aufzudecken.

88) Haefner S. 178; auch nach Bull, Ziele und Mittel, S. 13 sind wirksamere Sanktionen nötig.

89) Vgl. Roos S. 34.

90) Dies vermuteten bereits Anfang 1977 Blesgen und Weihe DB 1977 S. 437/438.

Besonders notwendig erscheint der strafrechtliche Schutz für den Bereich der Persönlichkeitsbilder, da hierin die Hauptgefahr der Datenverarbeitung gesehen werden muss [91]. Dieser Schutz vor "Persönlichkeitsprofilen" ist jedoch nur die zwangsläufige Folge, um die schon im Mikrozenzus-Urteil des BVerfG [92] gesehene Gefahr einer totalen Registrierung des Einzelnen zu bannen. Im Volkszählungsurteil wird auf diese Gefahr von Persönlichkeitsbildern nochmals mit Nachdruck hingewiesen [93]. Die Einführung der sog. "Neuen Medien" schließlich kann zur Anlegung umfangreicher Sammlungen personenbezogener Daten und damit Persönlichkeitsprofilen führen [94]. Allein der Bildschirmtext bietet "unerschöpfliche Möglichkeiten" solche Persönlichkeitsbilder anzulegen [95].

Zur wirksamen Verhinderung von Datenmißbrauch und insbesondere der Schaffung von Persönlichkeitsbildern ist damit grundsätzlich eine strafrechtliche Absicherungen erforderlich.

91) Haft DSWR 1979, 141 f.; ders. NJW 1979, 1197; Kamlah in: Burhenne/Perband § 41 RN 23. Für ein Verbot von Persönlichkeitsprofilen sind auch: Brödner S. 158; Bull, Ziele und Mittel, S. 44; Rissing-van Saan S. 252 f.; Weise DuD 1983, 70; Garstka JZ 1978, 511; Bull ÖVD 11/1979 S. 7. Die Profilbildung stellt nach Schneider, NJW 1984, 392, eine "neue Dimension der Gefahr" dar. Das französische Datenschutzgesetz (vgl. dazu § 2 B I der Arbeit) verbietet in seinem Art. 2 die Nutzung der aus Persönlichkeitsprofilen gewonnenen Daten. Nach Bull aaO ist eine Übernahme dieser Bestimmung "durchaus sinnvoll".

92) BVerfG 27, 1 ff.

93) BVerfG NJW 1984, 419, 421.

94) Leuze/Schedler/Schneider ÖVD 10/1980 S. 10; Alke DuD 1982, 90; Garstka DuD 1982, 153; 4. TB des BfD S. 9 f.

95) Bartl, Handbuch Btx-Recht, RN 199 (S. 177).

III) Standort und inhaltliche Erfordernisse einer Strafnorm

Wurde so die grundsätzliche Notwendigkeit einer (neuen) Strafnorm bejaht, so fragt sich weiter, wo sie angesiedelt werden muß. Das beste wäre, eine einheitliche Strafnorm zu schaffen [96] und diese im Kernstrafrecht (also dem StGB) [97], zu statuieren.[98]

1) Zur Begründung kann man zunächst einmal anführen, daß künftig weite Kreise der Bevölkerung mit EDV-Anlagen in Berührung kommen. War es vor Jahren noch einer Handvoll Spezialisten vorbehalten, mit Computern zu arbeiten, so hat nun zunehmend die Allgemeinheit, am Arbeitsplatz oder daheim, Zugriff auf EDV-Anlagen(Homecomputer, personal computer, Bildschirmtext). [99] Wird damit aber die Gefahr des Datenmißbrauchs größer, so steigt die Notwendigkeit einer für die Allgemeinheit verständlichen Strafnorm.

2) Die Aufteilung der datenschutzrechtlichen Strafbarkeit zwischen Bundesrecht und Landesrecht führt zu einem unerwünschten Partikularstrafrecht [100]. Die durch das Einführungsgesetz zum StGB vom 11.5.1973 intendierte größtmögliche "Einheitlichkeit des Strafrechts" [101] wurde mit den datenschutzrechtlichen Landesstrafnormen wieder aufgegeben. Dafür bestand kein sachlicher Grund, da keine "besondere regionale Bedürfnisse [102]" für die Schaffung angeführt werden können [103]. Datenverarbeitung macht weder Halt vor Landesgrenzen, noch sind die

96) Nach Naucke, Strafrecht, S. 127 liegt diese Überlegung nahe; ebenso Riemer bei Becker in: Schleswig-Holsteinische Anzeigen 1980 S. 32; a. A. wohl Zielinski, S. 153, der die Verletzungstatbestände typisieren und differenzieren will.

97) Lackner, StGB Vor § 1 Anm. 2; Roos S. 38: BT des StGB als Kernbestand des materiellen Strafrechts.

98) Naucke, Strafrecht, S. 127; Riemer bei Becker in: Schleswig-Holsteinische Anzeigen 1980, 32; vgl. auch Steinmüller in seinem Gutachten (BT-Drs. VI/3826 S. 62).

99) Rihaczek DuD 1980, 229.

100) Dazu Schönke-Schröder-Eser, Vor § 3 RN 47.

101) BT-Drs. 7/550 S. 197 u. S. 198;ebenso Schönke-Schröder-Eser, Vor § 1 RN 31 a; vgl. auch die Begründung im Bericht des Sonderausschusses zum EGStGB: BT-Drs. 7/1232 S. 1.

102) Jeschek S. 89.

103) Vgl. auch BT-Drs. 7/550 S. 197 f.

EDV-spezifischen Gefahren innerhalb der einzelnen Landsverwaltungen von unterschiedlicher Qualität oder Quantität.

Zudem geht gemäß § 7 II BDSG das Landesrecht insoweit vor, als der Datenschutz durch Landesgesetz geregelt ist. Die Bundesstrafnorm des § 41 BDSG gilt also nur subsidiär, während gegebenenfalls gleichfalls verwirklichte Strafnormen des StGB (wie z.B. §§ 203, 243, 303 StGB) den landrechtlichen Datenschutzstrafnormen vorgehen können. Diese kompetenzmäßig komplizierte Lage schafft indessen wenig Rechtsklarheit, womit eine bundeseinheitliche Gesamtregelung die praktikabelste und klarste Lösung des Problems wäre [104].

3) Weiterhin spricht der Charakter des BDSG als Auffanggesetz, d.h. subsidiäres Gesetz, dafür, eine einheitliche Norm im StGB zu schaffen. Durch jedes bereichsspezifische Datenschutzgesetz wird der Anwendungsbereich des § 41 BDSG (und der jeweiligen Landesstrafnorm) zunehmend kleiner [105]. Fraglich ist, ob diese Konsequenz vom Gesetzgeber bedacht worden ist, oder ob hier ungewollt lediglich verweisungsbedingte Straflücken entstehen.

Bereichsspezifische Gesetze haben gegenüber allgemeinen Gesetzen den Vorteil, differenziertere und sachnähere Regelungen zu statuieren. Bereichspezifische Strafgesetze laufen demgegenüber Gefahr, durch ihre Zersplitterung und "Aufstückelung" unübersichtlich und praktisch nicht realisierbar zu sein. Gerade wenn man

104) Schon 1972 hielt Steinmüller in seinem Gutachten (BT-Drs. VI/3826, S. 62) hinsichtlich der strafrechtlichen Fragen eine bundeseinheitliche Regelung für "dringend geboten"; vgl. auch soeben FN 98.

105) Solange nicht der Gesetzgeber eine (neue) Strafnorm schafft oder auf die Strafnorm des BDSG (bzw. der Landesgesetzgeber auf das LDSG) verweist; vgl. dazu oben, § 9 A IV 2) der Arbeit.

Allgemeinverständlichkeit von Strafgesetzen fordert [106], dürfen die Normen nicht unklar, verworren und komplex sein.

Die Bestrafung von Verstößen gegen bereichspezifische Gesetze ist auch durch eine einheitliche Norm möglich, wie ein Beispiel aus dem StGB verdeutlichen soll: So wird wegen Diebstahl betraft, wer eine fremde Sache wegnimmt. Bezüglich der Fremdheit sind nun außerhalb des StGB liegende Umstände heranzuziehen. Der Täter muß nur laienhaft wissen, daß ihm die Sache nicht gehört. Der Gesetzgeber hat hier verzichtet, bereichsspezifische Regelungen dergestalt zu treffen, daß einzeln festgelegt wird, ob Sicherungseigentum oder Sachen unter Eigentumsvorbehalt "fremd" sind und damit unter die Diebstahlsnormen fallen. Vielmehr hat er sich mit einer generellen Regelung begnügt.

Schafft man nun bereichsspezifische Gesetze so fördert man zwar die Individualgerechtigkeit, weil man sachgerechtere Regelungen statuieren kann. Strafrechtlich betrachtet wird dieses Ergebnis durch mangelnde Rechtsklarheit und Rechtssicherheit wieder aufgehoben. Eine allgemeine (generelle) Strafnorm im Kernstrafrecht kann indessen sowohl die Individualgerechtigkeit, als auch die Rechtssicherheit fördern.

Die Stellung im Kernstrafrecht würde nicht nur die Bedeutung der Strafnorm stärken ("Akzentuierungseffekt") [107], sondern auch ihre Publizität erhöhen. Der Gesetzgeber könnte die besondere Wichtigkeit dieses Deliktes für die Allgemeinheit hervorheben und ihre bessere Wirksamkeit garantieren, wie es

106) Haft DSWR 1979, 138: "Strafrecht muß einfach, anschaulich, verständlich und populär bleiben". Ähnlich: Baumann AT § 13 I. 3 (S. 154); ders. MDR 1958, 396; Kindermann S. 34; Lenckner JuS 1968, 305; Noll, Die Berücksichtigung der Effektivität, S. 144; Tiedemann NJW 1980, 1559; ders. Tatbestandsfunktionen, S. 197 f. und S. 242; Deubner NJW 1969, 623; aus der Rechtsprechung vgl. nur BayVerfGH in BayVGHE Bd. 67 (= Bd. 4 n.F.), S. 90, 106. Vgl. auch oben, § 3 A II 2) der Arbeit.

107) Bull 1. TB S. 65; des. betont in "Ziele und Mittel des Datenschutzes", S. 44, daß das Verbot von Persönlichkeitsprofilen "Appellfunktion" hätte.

z.B. auch bei der Überleitung der Konkursdelikte sowie der Kernenergie- und Strahlungsverbrechen aus dem Nebenstrafrecht in den "Kernbestand des materiellen Strafrechts" geschah [108]. Hier ist ferner daran zu erinnern, daß der im Entwurf zum BDSG vorgesehene § 33 ("Verletzung der Geheimhaltungspflicht") materiell ins StGB als § 203 II aufgenommen worden ist [109]. Auch für den dem jetzigen § 41 BDSG entsprechenden Paragraphen wurde erörtert, ihn ins StGB aufzunehmen [110].

Durch ihren Akzentuierungseffekt und ihre plakative Wirkung schafft eine einheitliche Norm im StGB des Bewußtsein einer Strafbarkeit des Datenmißbrauchs. Durch die Anknüpfung an die außerhalb des StGB liegenden Wertungen ermöglicht sie eine differenzierte und individuell angemessene Beurteilung.

4) Mit einer derartigen Strafvorschrift im StGB wäre es möglich auch Verstöße gegen bereichspezifische Gesetze zu erfassen. Deren Wertungen wurden dann über das Tatbestandsmerkmal "unbefugt" einfließen können. Desweiteren könnten dann die bereits bestehenden Strafnormen von bereichspezifischen Gesetzen gestrichen und somit weitere Nebenstrafrechtsnormen [111] abgebaut werden. Zudem bestünde einerseits für Bund und Länder, sowie andererseits für privaten und öffentlichen Bereich eine einheitliche Norm. Bei Verfahren aus dem öffentlichen Bereich konnte man den Eindruck gewinnen, erst durch die Datenschutzgesetze sei ein sorgfältiger(er) Umgang mit personenbezogenen Daten erreicht worden. Dies, obwohl doch schon immer Verschwiegenheits- und Amtspflichten bestanden. Eine Strafnorm im StGB könnte diesen positiven Effekt plakativ verstärken. Auch unter dem Gesichtspunkt

108) Roos S. 38/39.

109) So im Bericht des Innenausschusses, BT-Drs. 7/5277, "Zu § 33" (= S. 11).

110) Die entsprechende Vorschrift war § 32. Nach BT-Drs. 7/1027 "Zu § 32" (= S. 31), "bleibt zu prüfen, ob diese Strafvorschriften wegen ihrer allgemeinen Bedeutung in das StGB aufgenommen werden sollen". Aus den Materialien ist weder ersichtlich, warum dies dann doch nicht geschah, noch warum diese Überlegungen nicht zu Ende geführt wurden.

111) Naucke, Strafrecht, S. 125 schätzt die Zahl der strafrechtlichen Nebengesetze auf ca. 300. Es wäre eine eigene Untersuchung wert, diese Gesetze im Hinblick auf datenschutzspezifische Regelungen zu durchforsten.

verweisungsspezifische Fehler schon durch entsprechende Gesetzeskonstruktion zu vermeiden bietet sich eine einheitliche (Bundes-) Strafnorm an. Ein Überlesen der Verweisung auf die Strafbestimmungen der Ländergesetze oder auf den Anwendungsbereich wäre damit verhindert [112].

5) In bezug auf die inhaltliche Ausgestaltung der Strafnorm sind zwei Erfordernisse besonders wichtig:

So ist zum einen die Strafbarkeit der Vorbereitung und Schaffung von Persönlichkeitsbildern in die Sanktionsnorm aufzunehmen [113]. Dies folgt aus den oben ausgeführten Erörterungen zum "Quantitätskriterium" [114] und zur generellen Notwendigkeit einer Strafnorm [115].

Zum anderen sind die bei den Datenschutzgesetzen im Anwendungsbereich niedergelegten zentralen Voraussetzungen bei der neuen Norm als Tatbestandmerkmale zu statuieren. So verhindert z.B. die Nennung des Dateierfordernisses verweisungsbedingte Fehlverfügungen dergestalt, daß auch die Weitergabe aus (bloßen) Akten bestraft wird, mithin die Strafbarkeit über die Norm hinaus ausgedehnt wird.

112) Vgl. dazu ausführlich § 5 der Arbeit.

113) Siehe die Nachweise, oben FN 91.

114) Siehe oben, § 9 A VI der Arbeit.

115) Siehe oben § 9 B II der Arbeit.

IV) Reform der Strafverfolgungsvoraussetzungen

Neben diesen Strafbarkeitsanforderungen an eine neue Sanktionsnorm gilt es auch die Strafverfolgungsvoraussetzungen zu überprüfen. Diskutiert werden sollen zwei mit dem Strafantragsrecht zusammenhängende Reformüberlegungen:

-Erstens, ob man den Datenschutzbeauftragten in Bund und Ländern generell ein Strafantragsrecht zugestehen sollte [116].

-Zweitens, ob man den Staatsanwaltschaften bei Vorliegen eines öffentlichen Interesses die Möglichkeit des Einschreitens eröffnen sollte [117].

1) Strafantragsrecht der Datenschutzbeauftragten:

Einerseits könnte man dem Bundesbeauftragten für den Datenschutz (BfD) und auch den übrigen Datenschutzbeauftragten der Länder, die bisher kein solches Recht hatten, die Strafantragsbefugnis zugestehen [118]. Andererseits wäre auch möglich die bisher bestehenden Befugnisse abzuschaffen [119].

a) Als Begründung für die Schaffung des Strafantragsrechts des baden-württembergischen Landesdatenschutzbeauftragten findet sich in der Gesetzesbegründung des Landtages folgende Formulierung [120]:

116) Bull, 5. TB des BfD (= BT-Drs. 9/2386) S. 115, empfiehlt "zur Abrundung" ein Strafantragsrecht des BfD.

117) So die entsprechenden Überlegungen eines DVD-Arbeitskreises (DANA 5/1979 S. 19 = DVD-Jahrestagung 1979, S. 169). Bereits jetzt besteht diese Lösung in § 21 III NDSG.

118) Bull, 5. TB des BfD (= BT-Drs. 9/2386) S. 115.

119) So empfiehlt Tegtmeyer, ÖVD 1981, 13, eine "Überprüfung" der bestehenden Strafantragsrechte.

120) Landtag Baden-Württemberg, LT-Drs. 7/2550 S. 52 ("Zu § 26").

"In Abweichung von § 41 BDSG wurde auch dem Landesbeauftragten für den Datenschutz ein Strafantragsrecht eingeräumt. Es stellt eine sinnvolle Ergänzung der Aufgaben und Rechte dar, die dem Landesbeauftragten für den Datenschutz im Interesse einer wirksamen Überwachung des Datenschutzes eingeräumt sind."

Treffender als das Argument der "sinnvollen Ergänzung" dürfte freilich das der Sachnähe sein. Die Datenschutzbeauftragten sind rechtlich und fachlich am besten geeignet und haben die größte Erfahrung aufgrund ihrer Kontrolltätigkeit. Desweiteren spricht für ein Antragsrecht, daß ihnen wohl von den Betroffenen das größte Vertrauen entgegengebracht wird. Besonders in den Fällen, in denen sich der Einzelne scheut, selbst aktiv gegen eine für ihn übermächtige Verwaltung oder Organisation vorzugehen, könnte hier der Datenschutzbeauftragte durch seinen Antrag dem Betroffenen helfend zur Seite stehen. Auch könnte er in den Fällen, in denen ein Betroffener nicht zu ermitteln ist, verhindern, daß allein der Zufall oder aber die besondere Gerissenheit des Täters zur Straflosigkeit führt. Weiterhin könnte er bei Verstössen in sicherheitsempfindlichen Behörden (z.B. Verfassungsschutz) tätig werden und ohne Einschaltung der Betroffenen eine Strafverfolgung der Täter erreichen. Schließlich ist das Strafantragsrecht als ein wirksames Druckmittel bei den Kontrollen der Datenschutzbeauftragten anzusehen (wenigstens innerhalb der 3-Monatsfrist des § 77 d StGB). Auch die Beratungsfunktion der Datenschutzbeauftragten würde durch ein Strafantragsrecht nicht beeinträchtigt, da der Datenschutzbeauftragte auch jetzt schon über eine Anzeige und/oder

Unterrichtung des Betroffenen ein Ermittlungsverfahren in Gang bringen kann [121].

b) Gegen ein Strafantragsrecht spricht zunächst die Möglichkeit von Kollisionen zwischen dem Antrag des Datenschutzbeauftragten und dem des Betroffenen. Es kann nämlich der eine eine Strafverfolgung be-"antragen", der andere aber nicht bzw. sogar ausdrücklich nicht. Da das BDSG indessen vom Schutz der Privatsphäre des Betroffenen als Schutzzweck ausgeht, muß hier eine Entscheidung zugunsten des Betroffenen ausfallen: Seinem Willen gebührt der Vorrang. Er muß grundsätzlich gegenüber einem ebenfalls strafantragsberechtigen Datenschutzbeauftragten verhindern können, durch einen gegen seinen Willen durchgeführten Strafprozeß erneut in schutzwürdigen Belangen verletzt zu werden [122]. Nötig wäre somit eine Konstruktion des Strafantragsrechts der Datenschutzbeauftragten, die eine Zustimmung des Betroffenen zur Voraussetzung hat [123]. Problematisch ist diese Lösung jedoch in den Fällen, in denen die Betroffenen unbekannt blieben. Um aber sie und die Fälle der Antragskollission zu erfassen, könnte man nicht die Zustimmung des Betroffenen verlangen, sondern keinen entgegenstehenden Willen, d.h., der Strafantrag des Datenschutzbeauftragten

121) Hierbei ist allerdings umstritten, ob die Datenschutzbeauftragten in Bund und Ländern verpflichtet sind, die Aufsichtsbehörden und/oder den Betroffenen zu unterrichten. Während nach § 21 V LDSG SH der Landesbeauftragte ausdrücklich befugt ist, den Betroffenen zu unterrichten, will z. B. Dammann (in: Simitis/D/M/R § 41 RN 34) grundsätzlich nur eine Unterrichtung der Aufsichtsbehörde gestatten. Am sinnvollsten dürfte das sein, was auch die Bundesregierung auf eine kleine Anfrage des Abgeordneten Laufs (BT-Drs. 8/206 Frage B 25 vom 21.3.1977, S. 1393 f.) geantwortet hat, nämlich daß zumindest bei schwerden Verstößen die Pflicht gegenüber beiden besteht. Nur so kann der Schutz des Betroffenen, der Sinn und Zweck des Gesetzes (und damit auch der Institution des Datenschutzbeauftragten) ist, wirksam erreicht werden. Dies gilt um so mehr, als daß das BVerfG "der Beteiligung unabhängiger Datenschutzbeauftragter erhebliche Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung" zuerkennt (BVerfG NJW 1984, 419, 422/423).

122) So Auernhammer, Kommentar, § 41 RN 10; Dammann in: Simitis/D/M/R § 41 RN 34 und Kutzmann Anm. 7 zu § 27 LDatG RP. Dagegen spricht allerdings, daß gemäß § 172 GVG die Öffentlichkeit ausgeschlossen werden kann, wenn durch die Erörterung der persönliche Lebensbereich oder privater Geheimnisse schutzwürdige Belange verletzt werden (vgl. § 172 Nr. 2 und Nr. 3 GVG).

123) So bereits in Nordrhein-Westfalen (§ 37 III 2 LDSG NW).

kann nur durch einen ausdrücklichen Verzicht des Betroffenen zu Fall gebracht werden. Rechtsdogmatisch ließe sich dies durch eine Art "Stellvertretervermutung" erklären: Der Datenschutzbeauftragte darf zunächst "für den Betroffenen" Strafantrag stellen, dieser kann aber dann durch seinen Verzicht ihm die Befugnis wieder entziehen.

Doch selbst gegen diese Konstruktion bestehen grundsätzliche Bedenken: Der Anwendungsbereich der Befugnisse der Landesdatenschutzbeauftragten ist auf die öffentliche Verwaltung eines Landes beschränkt. Durch die Gewährung eines Strafantragsrechts sind somit die Täter aus diesem Bereich poteniell schlechter gestellt. Besonders in den Fällen, in denen Betroffene nicht zu ermitteln sind, kann somit eine Verurteilung davon abhängen, "für wen der Computer arbeitet". Angesichts der oft schwierigen und manchmal wahrscheinlich unmöglichen Abgrenzung des Anwendungsbereichs des Landes- und Bundesdatenschutzgesetzes [124] wird es für den Beschuldigten höchst zufällig, ob er bestraft wird. Für eine Differenzierung zwischen Bundes- und Landesverwaltung ist zudem kein sachlich vernünftiger Grund ersichtlich, denn Anknüpfungspunkt waren die Kompetenzverteilungen und nicht die computerspezifischen Gefahren. Doch selbst wenn man zusätzlich dem Bundesdatenschutzbeauftragten ein Antragsrecht einräumte und damit für die Bundesverwaltung zu einer Angleichung käme, bliebe eben immer noch die computerunspezifische Differenzierung zwischen öffentlichem und privatem Bereich. Die Datenschutzgesetze bezwecken, den Mißbrauch bei der Datenverarbeitung und nicht bei der "Aktenverarbeitung" zu verhindern. Dieser Zweck fordert aber keine Differenzierung zwischen privatem Bereich einerseits und öffentlichem andererseits.

124) Vgl. dazu die oben dargestellte Verweisungskomplexität, § 3 B der Arbeit.

Gegen ein Antragsrecht der Datenschutzbeauftragten sprechen jedoch auch die aus dem Sinn und Zweck eines Antragsrechtes folgenden Überlegungen. So kann ein Betroffener als Verletzter frei entscheiden. Sein "Motiv ist gleichgültig" [125]. Der Datenschutzbeauftragte indessen darf dieses Recht nicht nach seinem persönlichen Belieben ausüben, sondern er muß sachgerechte Erwägungen anstellen, wie z.B. das Interesse des Betroffenen an einer Strafverfolgung. Dabei ist allerdings zu bedenken, daß diese Entscheidung des "Staatsorgan Datenschutzbeauftragter" weder gerichtlich noch sonst von einer übergeordneten Instanz nachprüfbar ist. Doch nicht allein die Möglichkeit völlig frei und ohne Kontrolle entscheiden zu können, spricht gegen ein Strafantragsrecht. Das gewichtigste Gegenargument ist, daß die ansonsten nur überwiegend präventiv tätigen Datenschutzbeauftragten mit der Erörterung des "öffentlichen Interesses" im Sinne einer Strafverfolgung repressive und originär staatsanwaltliche Tätigkeiten ausüben. Dies bedeutet einen Systembruch. Es ist kein Grund ersichtlich, einem Nicht-Verletzten ein Antragsrecht zuzugestehen. Die größere Sachnähe als Begründung ansehen dürfte verfehlt sein, da man ansonsten sämtlichen Spezialbehörden, die komplizierte Gesetze zu überwachen oder auszuführen haben, ein solches Antragsrecht ebenfalls zubilligen müßte [126].

Gegen ein Strafantragsrecht spricht schließlich der hier vorliegende empirische Befund [127]. Wenn bisher in 5 Jahren nur in einem einzigen Fall das Strafverfahren durch Anzeige von einem Datenschutzbeauftragten eingeleitet wurde und in keinem der Verfahren ein Strafantrag gestellt wurde, so ist das ein gewichtiges Indiz für die praktische Bedeutungslosigkeit eines

125) Dreher/Tröndle § 77 RN 30.

126) Den für das Weinrecht zuständigen Behörden hat man auch nicht ein Strafantragsrecht eingeräumt, obwohl die Vorschriften zum Weinrecht mit ihrem Umfang und Komplexität die der Datenschutzgesetze vielleicht sogar noch übertreffen; vgl. dazu A. Schnell, Diss. Tübingen 1984.

127) Siehe oben, § 8 II 1 der Arbeit und dort die Tabelle 8.2 "Strafantragsmöglichkeit der LfD".

solchen Rechts. Also sprechen auch die (Rechts-) Tatsachen gegen ein Strafantragsrecht.

c) Zusammenfassend läßt sich feststellen:
Ein Strafantragsrecht der Datenschutzbeauftragten in Bund und Ländern ist empirisch überflüssig und de lege ferenda nicht wünschenswert; die bisherigen Strafantragsrechte sind bedenklich und daher zu streichen [128].

2) Öffentliches Interesse:

Zu erörtern bleibt die "niedersächsische Lösung", nämlich zusätzlich zum Strafantragsrecht des Betroffenen die Staatsanwaltschaft bei Vorliegen eines besonderen öffentlichen Interesses zur Strafverfolgung zu ermächtigen.

a) Gegen eine solche Lösung spricht zunächst nur, daß damit gegen die Belange des Betroffenen verstoßen werden könnte [129]. Denn wendet er sich gegen eine Strafverfolgung, da er eine erneute Verletzung seiner Privatsphäre durch ein Strafverfahren verhindern will, so würde das die Staatsanwaltschaft nicht hindern die Strafverfolgung zu betreiben. Allerdings ist hier zweierlei zu bedenken:

Zum anderen sieht auch das geltende Recht ein Nebeneinander von Strafantragsrecht und öffentlichem Interesse vor, wie z.B. bei den Körperverletzungsdelikten der §§ 223, 230 StGB oder bei § 183 StGB (Exhibitionistische Handlungen) [130]. In beiden Fällen sind höchstpersönliche Rechtsgüter [131] wie die körperliche

128) Auch Tegtmeyer, ÖVD 1981 S. 13, empfiehlt eine "Überprüfung" der Strafantragsrechte durch die jeweiligen Landesgesetzgeber.

129) So Bautsch Anm. 2 zu § 21 NDSG.

130) Bei den Körperverletzungsdelikten nach § 232 I StGB, bei exhibitionistischen Handlungen nach § 183 II StGB.

131) Zum Begriff "höchstpersönliches Rechtsgut": Schönke-Schröder-Stree, Vor § 52 RN 43 ff.

und psychische Integrität betroffen [132]. Somit ist ein Vergleich mit den Datenschutzgesetzen möglich, da dort die "schutzwürdigen Belange eines Betroffenen" [133] und damit ebenfalls höchstpersönliche Rechtsgüter betroffen sind. Damit kann aber auch ein mögliches Nebeneinander von Strafantrag und öffentlichem Interesse nicht als Argument gegen die "niedersächsische Lösung" angeführt werden.

b) Für eine solche Erweiterung spricht indessen, daß damit all die Fälle erfaßt werden könnten, in denen der Betroffene unbekannt geblieben ist. Auch wäre eine Strafverfolgung dann möglich, wenn der einzelne Betroffene sich zwar einerseits scheut, selbst einen Strafantrag zu stellen, andererseits aber auch nichts gegen eine Strafverfolgung durch die Staatsanwaltschaft einzuwenden hätte. Ferner könnte durch eine solche Novellierung sowohl eine Gleichstellung zwischen öffentlichem und privaten Bereich, als auch zwischen Bundes- und Landesverwaltung erreicht werden. Desweiteren ließe sich damit verhindern, daß Verfahren nur wegen verspätet gestellten Strafanträgen eingestellt werden müssen [134].

3) Zusammenfassend läßt sich festhalten:

Bei allen Datenschutzgesetzen sollte die Regelung des § 21 III NDSG übernommen werden; auch die Strafverfolgungsbehörden sollten bei besonderem öffentlichen Interesse von Amts wegen tätig werden können [135].

132) Nach Lackner, Anm. 1 zu § 183 StGB, schützt § 183 StGB die "psychische und körperliche Intergrität". Auch nach Schönke-Schröder-Lenckner, § 183 StGB RN 2, ist durch § 183 StGB der Schutz des einzelnen bezweckt (ebenso Dreher, § 183 StGB RN 2); zum Schutzgut der Körperverletzungsdelikte: Schönke-Schröder-Eser, § 223 RN 1 und Dreher, § 223 RN 1.

133) Diese zu schützen ist nach § 1 I 1 BDSG "die Aufgabe des Datenschutzes".

134) Vgl. von den hier vorhandenen sieben Verfahren nur den im Anhang vorgestellten Fall 10 ("Jugendstrafe"). Bei den Fällen der "Auskunftserschleichung" von Auskunfteien bestand die Gefahr verspäteter Strafanträge besonders oft.

135) So auch die Überlegungen eines DVD-Arbeitskreises: DANA 5/1979 S. 19 = DVD-Jahrestagung 1979 S. 169. Rieß, Gutachten, C 70, RN 98, schlägt vor, daß bei Antragsdelikten generell auch eine Strafverfolgung bei Vorliegen eines besonderen öffentlichen Interesses eingeführt werden sollte.

V) Eigener Vorschlag für eine Strafnorm

Der eigene Vorschlag einer Strafvorschrift beschränkt sich auf die Novellierung einer datenschutzrechtlichen Sanktionsnorm im StGB. Nötig wäre als zweiter Schritt eine Überarbeitung von § 203 StGB. Da jedoch schon das dogmatische Verhältnis der Delikte zueinander ausgeklammert werden mußte [136], gilt dies um so mehr für eine zu entwerfende Neufassung des § 203 StGB. Mein Vorschlag für eine datenschutzrechtliche Strafnorm lautet:

§ 206 StGB(Datenschutz-Verletzung(1)):

1) Wer (2) unbefugt (3) personenbezogene Daten (4) in einer Datensammlung (5) speichert (6), aus ihr weitergibt (7) oder sich aus ihr solche verschafft (8) und dadurch das informationelle Selbstbestimmungsrecht (9) eines anderen erheblich (10) beeinträchtigt wird mit Geldstrafe oder Freiheitsstrafe bis zu einem Jahr bestraft.

2) In besonders schweren Fällen wird Datenmissbrauch mit Geldstrafe oder Freiheitsstrafe bis zu zwei Jahren bestraft. Ein besonders schwerer Fall liegt in der Regel vor, wenn Persönlichkeitsbilder (11) vorbereitet (12) oder geschaffen werden.

3) Der Täter handelt unbefugt, wenn er ohne ausdrückliche Einwilligung des Betroffenen oder Erlaubnis durch Gesetz handelt.

4) Die Tat wird nur auf Antrag des Betroffenen oder bei Vorliegen eines besonderen öffentlichen Interesse an der Strafverfolgung (13) verfolgt.

136) Vgl. dazu § 1 (Einleitung) der Arbeit.

Begründung des eigenen Vorschlages

Im folgenden werden die Gründe für diese Fassung der Norm angegeben, wobei die Wortwahl im einzelnen erläutert wird:

(1) Datenschutz-Verletzung:

Besser wäre zwar, von "Verdatungsschutz" zu sprechen, da sich der Ausdruck "Datenschutz" jedoch eingebürgert hat, ist er zu verwenden.

(2) Wer:

Damit kann Täter jedermann sein. Zudem wird das Problem vermieden, daß die Datenschutzgesetze von "Stellen" sprechen, das Strafrecht aber auf Personen zugeschnitten ist [137].

(3) unbefugt:

Die "Unbefugtheit" sollte als Tatbestandsmerkmal gelten, um so legale Handlungsweisen bereits auf Tatbestandsebene ausscheiden zu können. Der rechtliche Unwertcharakter der Handlung entsteht erst durch deren unbefugte Vornahme [138]. Ein weiterer Vorteil wäre, daß man so bei jeder Handlung dem Beschuldigten den Verstoß gegen eine konkrete Norm vorzuhalten gezwungen ist, was zudem verhindert, daß der Anwendungsbereich konturenlos wird. Die "Tatbestandslösung" rechtfertigt sich auch aus der Auswertung: Bei vielen Verfahren mußte man oft den Eindruck haben, daß Staatsanwälte der Meinung waren, daß etwas verboten sei, "weil es eben verboten ist", sich aber keine Gedanken über die konkrete Verbotsnorm machten.

137) Haft DSWR 1979, 140; ders. NJW 1979, 1195 f.; ähnlich Marx DSWR 1979, 87 und Kamlah in:Burhenne/Perband § 41 RN 9.

138) Warda JURA 1979, 295.

(4) personenbezogene Daten:

Der Begriff hat sich zum einen eingebürgert, zum anderen ist "personenbezogene" Daten besser (da umfassender) als "persönliche" Daten.

(5) Datensammlung:

Obwohl die Beschränkung der Datenschutzgesetze auf Dateien als unzweckmäßig (teilweise sogar als falsch) angesehen wird [139], ist grundsätzlich an einer an den Gefahren der EDV anknüpfenden Einschränkung festzuhalten, da sonst hier im Strafrecht die Gefahr bestände, daß ein allgemeines Indiskretionsdelikt geschaffen wird. Neben dem Begriff "Datensammlung" könnte man auch den Begriff "Datenspeicher" wählen. Besonders "Datensammlung" hat jedoch gegenüber "Datei" den Vorteil, daß dieser Begriff nicht aus der Fachsprache der EDV stammt, mit der nicht nur die meisten Juristen (noch?) ihre Probleme haben. Ferner ist damit sowohl die Einbeziehung von Karteien, Mikrofiches und ähnlichem möglich, als auch die Erfassung unformatierter Daten in EDV-Anlagen (Stichwort "Textverarbeitung") [140] gewährleistet.

(6) speichern:

Da die Gefährdung erst mit der Speicherung beginnt [141], erscheint eine Einbeziehung der Datenerhebung in eine Strafnorm nicht geboten [142]. Es sollte deshalb, wie bisher schon in einigen Landesdatenschutzgesetzen [143], nur die Speicherung sanktions-

139) So wohl jetzt Simitis NJW 1984, 402.

140) Vgl. dazu Weise DuD 1980, 139 ff.

141) Bull/Zimmermann FuR 1979, 122.

142) Rissing-van Saan S. 76. Die Mehrheit der Datenschutzkommission des Deutschen Juristentages wollte den Schutz schon an die Sammlung personenbezogener Daten anknüpfen (S. 24). Für eine Einbeziehung sogar schon der Erhebung wohl Simon/Taeger JZ 1982, 141. Leuze/Schedler/Schneider, ÖVD 10/1980 S. 16, fordern ein strafrechtlich abgesichertes Verbot der Erhebung personenbezogener Daten durch die Anbieter im Bereich der Neuen Medien.

143) § 30 I Nr. 1 BrDSG; § 23 I Nr. 1 LDSG SH und nach der Kommentierung von Kutzmann (Erl. 3) auch § 27 LDatG RP.

bewehrt sein [144].

(7) weitergibt:

Wie bereits oben dargelegt [145], ist der Begriff "weitergeben" dem von "übermitteln" vorzuziehen.

(8) "Verschaffen":

Dieser Terminus erfaßt sowohl abrufen als auch sonstiges verschaffen und verhindert durch den gleichzeitigen Verzicht auf das einschränkende Merkmal "aus in Behältnissen verschlossenen Dateien", die sich bisher daraus ergebenden Friktionen [146].

(9) informationelles Selbstbestimmungsrecht:

Hiermit können die vom BVerfG im Volkszählungsurteil ausgeführten Wertungen berücksichtigt werden [147]. Das dagegen scheinbar anzuführende Argument einer Generalklausel verkennt, daß diese dem strafrechtlichen Bestimmtheitsgebot nicht eo ipso entgegenstehen, wie z. B. die Unangefochtenheit des § 185 (Beleidigung) zeigt.

(10) erheblich:

Mit Hilfe dieses Merkmals ist es möglich, belanglose Verstöße auszuscheiden und zudem dem Gesichtspunkt des "Quantitätskriteriums" [148] Rechnung zu tragen.

144) Für eine strafrechtliche Sanktionierung der Speicherung: Garstka DuD 1981, 156; Leuze/Schedler/Schneider ÖVD 10/1980 S. 12; Schneider in: Gallwas/S/S § 41 RN 2; Schweinoch/Geiger Einl. zum BayDSG S. 23; Louis RN 351 und Rissing-van Saan S. 269; Gallwas, Der Staat 1979, S. 518; a. A. Auernhammer, Kommentar, § 41 RN 2, nach dem das Speichern strafrechtlich vernachlässigt werden kann.

145) § 7 B III der Arbeit.

146) § 7 B I u. II der Arbeit.

147) BVerfGE 65, 1 ff. = NJW 1984, 419 ff.

148) Siehe oben, § 9 A VI der Arbeit.

(11) Persönlichkeitsbilder:

Durch die ausdrückliche Nennung dieses Beispiels soll der leitende Gedanke für den wichtigsten Grund der Strafnorm hervorgehoben werden [149]. Die Bezeichnung "Persönlichkeitsbilder" entspricht der Terminologie des BVerfG [150]. Möglich wäre auch Datenbilder oder Persönlichkeitsprofile, während der Begriff "Datenschatten" zu konturenlos ist.

(12) vorbereitet:

Damit findet für den besonders gefährlichen Bereich der Persönlichkeitsbilder eine Vorverlagerung in den Versuchsbereich statt, der ansonsten ungeschützt bleiben kann.

(13) öffentliches Interesse:

Bereits oben wurde ausführlich dargelegt, warum auch bei Vorliegen eines öffentlichen Interesses eine Strafverfolgung möglich sein sollte [151].

149) Für ein Verbot: Brödner S. 158; Bull, Ziele und Mittel, S. 44, der die "Appellfunktion" eines solchen Verbotes betont; ders. ÖVD 11/1979 S. 7; Haft DSWR 1979, 141; ders. NJW 1979, 1197; Rissing-van Saan S. 252 f.; Weise DuD 1983, 70; wohl auch Garstka JZ 1978, 511; Kamlah in: Burhenne/Perband § 41 RN 23.

150) BVerfGE 65, 1 ff. = NJW 1984, 419 ff.

151) Siehe § 9 B IV der Arbeit.

ANHANG

FÄLLE

Fall 3 ("Einkommenshöhe"):

Zwischen dem Anzeigenerstatter A und seiner geschiedenen Frau schwebte ein Unterhaltsstreit. Der Arbeitgeber T des A wurde deshalb vom Gericht gebeten, das Einkommen des A mitzuteilen. Nach anderen Streitigkeiten zwischen T und A wurde das Arbeitsverhältnis (nach arbeitsgerichtlichen Auseinandersetzungen) gelöst. Einige Zeit später teilte T dem mit der Unterhaltsstreitigkeit befaßten Gericht mit, "daß bei einer Überprüfung der Personalakte festgestellt worden sei, daß das tatsächliche Einkommen des A höher gelegen habe". Eine gleichlautende Mitteilung erhielt seine geschiedene Frau. Der Staatsanwalt stellte bezüglich der Weitergabe an das Gericht das Verfahren gegen T ein. Im Hinblick auf die Weitergabe an A's geschiedene Frau sei die Schuld gering, so daß wegen des hier vorliegenden Verstoßes gegen das BDSG das Verfahren nach § 153 I StPO einzustellen sei. Nach Zustimmung durch das Gericht geschah dies auch.

Fall 4 ("Taxifahrer"):

Student S stellte einen Antrag auf Erteilung einer Taxikonzession. Im Rahmen des Verfahrens wurde gemäß § 14 PBefG als Berufsvertretung die Taxi-Innung e.V. gehört und ihr dafür die nötigen personenbezogenen Daten über S zur Verfügung gestellt. Einige Tage später erhielt S von einer Versicherungsvermittlungs-GmbH auf ihn zugeschnittene Angebote zum Abschluß von Versicherungen im Zusammenhang mit einer Taxikonzession. Nach erfolglosen Beschwerden bei der Innung und der GmbH wandte er sich an die nach § 30 BDSG zuständige Aufsichtsbehörde und stellte "Strafantrag nach § 41 BDSG". Die Aufsichtsbehörde setzte sich mit dem Landesdatenschutzbeauftragten in Verbindung und beide kamen zum Ergebnis, daß die Übermittlung nach § 24 BDSG zu beurteilen sei. Ferner sei davonauszugehen, daß "die Innung in Ausführung des § 14 PBefG nicht als beliehener Unternehmer handelt - mangels der Möglichkeit von Zwangsmaßnahmen - und damit nicht als "sonstige öffentliche Stelle" des Landes anzusehen sei". Bei den weiteren Ermittlungen stellte sich heraus, daß S nie Mitglied der Innung war und somit die Übermittlung gemäß § 24 BDSG als unzulässig anzusehen sei. Desweiteren wurde offenbar, daß Taxifahrer T sowohl Vorsitzender der Innung, als auch Geschäftsführer der GmbH war. T verweigerte jegliche Angaben zur Sache. Das Verfahren wurde darauf nach § 153 a StPO unter Auferlegung einer Geldbuße von 500 DM eingestellt, mit der Begründung, es liege ein Verstoß gegen "das Datenschutzgesetz" vor, da "unbefugt personenbezogene Daten, die nicht offenkundig seien, an einen Dritten übermittelt worden seien, indem T als Vorsitzender der Innung Daten des S ohne dessen Zustimmung an die GmbH weitergegeben habe". Im internen Vermerk der StA wurde ausgeführt, daß T wohl einem vermeidbaren Verbotsirrtum unterlegen sei, und, daß sich die Höhe des auferlegten Betrages von 500 DM daraus ergebe, daß nicht mehr als 30 Tagessätze zu erwarten seien.

Fall 5 ("Vorstandsvorsitzender"):

Der Vorstandsvorsitzende V einer AOK schrieb kurz vor Weihnachten 1980 einem Minister, nach dessen kritischen Reden über den Mißbrauch des sozialen Sicherungssystems, einen Brief, in dem er unter voller Namensnennung des B das "unverschämte Ausnutzen des sozialen Netzes" durch einen "Privilegierten" anprangerte, zu dem ein "gewöhnlicher Arbeitnehmer moralisch nicht in der Lage" wäre. Danach schilderte er den Fall des B (der Mitglied der AOK war) in allen Einzelheiten. Einen Durchschlag des Briefes übersandte er der Lokalzeitung L mit der Bitte, den Namen bei einer Veröffentlichung wegzulassen. Ferner begründete er sein Schreiben an den Minister kurz vor Weihnachten der L gegenüber wie folgt: "Ab 1.1.1981 tritt nämlich das Datenschutzgesetz in Kraft und ich könnte dann den Namen nicht mehr nennen." So wurde der Brief Tage später ohne Namensnennung aber im vollen Wortlaut abgedruckt. Dennoch wurde einem Teil der Einwohner sofort klar, daß nur B gemeint sein konnte und er wurde schon am Erscheinungstag der Zeitung darauf angesprochen. Der Anwalt des B stellte daraufhin Strafantrag "wegen Beleidigung, Geheimnisverrat (§ 203 II Nr. 1 und 2 StGB), sowie § 41 I BDSG". Dabei sei der strafschärfende Tatbestand des Handelns zum Schaden eines anderen zu beachten (§ 203 V StGB, § 41 II BDSG) und zu berücksichtigen, daß bei Daten aus dem medizinischen Sektor ein besonderes Interesse an der Geheimhaltung bestehe.

Als der ebenfalls informierte Landesdatenschutzbeauftragte bei der AOK anfragte, antwortete diese, daß alle Angaben aus Unterlagen entnommen seien, die nicht dem Landesdatenschutzgesetz unterfielen.

Bei den Ermittlungen stellte sich heraus, daß Daten (die zum Teil falsch waren) über B "teils aus den bei der AOK geführten Karteien, teils aus gespeicherten Datenträgern entnommen und auf einem DIN-A-4-Blatt zusammengestellt" waren. Name, Geburtsdatum, Wohnanschrift, Versicherungsarten und Arbeitslosengeldbezug waren über Datenträger gespeichert, die übrigen Daten aus den bei der AOK geführten Dateien entnommen. Weitere Daten stammten aus Heil- und Kostenplänen. V hatte die Daten von dem von ihm beauftragten Angestellten A der AOK übernommen, ohne sie auf ihren Wahrheitsgehalt zu überprüfen.

V räumte den ihm zur Last gelegten Sachverhalt im wesentlichen ein, hielt jedoch sein Vergehen für rechtmäßig. Seine Entscheidung sei das Ergebnis einer Güterabwägung der in Konflikt geratenen Interessen. Er sei nicht nur berechtigt, sondern verpflichtet gewesen, im Interesse der Solidargemeinschaft der Versicherten der AOK und im Interesse der Allgemeinheit zu handeln und mit diesem Fall an die Öffentlichkeit zu gehen. Außerdem verstehe er unter Schutz der Sozialdaten nur den der medizinischen, nicht der versicherungstechnischen Daten.

Gegen den Angestellten A wurde von der Staatsanwaltschaft kein Ermittlungsverfahren eingeleitet, mit der Begründung:

"A war dem V gegenüber dienstlich verpflichtet, die Unterlagen zur Verfügung zu stellen. Er hat daher nicht unbefugt gehandelt im Sinne von § 203 StGB, der § 41 BDSG als lex specialis vorgeht. ...Zudem hat er nicht mit dieser Handlungsweise des V rechnen müssen." Gegen den nicht vorbestraften V wurde ein Strafbefehl in Höhe von 20 Tagessätzen wegen §§ 203 II Nr. 1, 185, 52, 40 StGB beantragt. Der zuständige Richter hatte jedoch

Bedenken und ordnete die Durchführung einer Hauptverhandlung gemäß § 408 II StPO an. Der Strafbefehl wurde deshalb V gemäß § 408 Abs. 2 ohne beantragte Rechtsfolge zugestellt.
Kurz vor der angesetzen Hauptverhandlung im September 1981 erschien im "Spiegel" ein Bericht über den Fall mit voller Namensnennung des B. Daraufhin erstattete B erneut Strafantrag wegen Verletzung des Privatgeheimnisses und Verstoßes gegen § 35 I SGB I. Mitte Oktober 1981 fand die Hauptverhandlung vor dem Amtsgericht statt.

V wurde wegen Verletzung von Privatgeheimnissen zu einer Geldstrafe von 15 Tagessätzen verurteilt. In seiner Begründung führte das Gericht aus: "Nach dem festgestellten Sachverhalt hat sich der Angeklagte V der Verletzung von Privatgeheimnissen nach § 203 StGB schuldig gemacht. Der Angeklagte hat in seiner Funktion als Vorstandsvorsitzender der AOK und damit als Amtsträger im Sinne des § 203 Abs. 2 Ziff. 1 StGB fremde Geheimnisse, die ihm in seiner Funktion als Vorstandsvorsitzender der AOK bekannt geworden sind, unbefugt offenbart." Es erörterte dann ausführlich mögliche Rechtsfertigungs- und Entschuldigungsgründe, die jedoch verneint wurden. Weiter heißt es: "Zugleich liegt ein Verstoß gegen § 41 Bundesdatenschutzgesetz vor. Der Angeklagte hat unbefugt die vom BDSG geschützten personenbezogenen Daten, die nicht offenkundig waren, weitergegeben. Hierbei spielt es keine Rolle, ob die übermittelten Daten aus einem für die automatisierte Datenverarbeitung benutzbaren Datenträger (Lochkarten, Magnetband, Magnetplatte) oder aus losen Karteikarten, wie sie bei der konventionellen Datenverarbeitung benutzt werden, stammten. Für die Geltung des BDSG ist es unerheblich, in welchem Verfahren personenbezogene Daten verarbeitet werden, ob automatisch oder manuell (vgl. Simitis/Dammann/Mallman, Kommentar zum BDSG, 1. Aufl. § 1, RNr. 26; § 2 Anm. 187; Burhenne/Perband, Kommentar zum BDSG § 2, RNr. 116, 119). Der Begriff der Datei im Sinne des BDSG ist somit wesentlich weiter, als er in der Terminologie der Informatik üblicherweise verstanden wird. Er setzt lediglich voraus, daß die Sammlung von Daten nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden kann.

§ 203 StGB geht als die Vorschrift, die denselben Sachverhalt enger begrenzt und spezieller ausgestaltet, dem § 41 BDSG als "lex specialis" vor (vgl. Dreher/Tröndle, Kommentar z. StGB, 40. Aufl., Anm. 9 a zu § 203)."

Nachdem V und B Berufung eingelegt hatten, fand erneut eine Hauptverhandlung statt, in der V darauf hingewiesen wurde, daß auch eine Verurteilung wegen übler Nachrede erfolgen könne. Es erging durch das Landgericht folgendes Urteil:

"Der Angeklagte V ist eines Vergehens der Verletzung von Privatgeheimnissen, begangen in Tateinheit mit einem Vergehen der üblen Nachrede, schuldig.
Er wird hierwegen verwarnt.
Die Verurteilung zu einer Geldstrafe von 20 Tagessätzen zu je ... DM bleibt vorbehalten. ... Angewandte Vorschriften: §§ 203 Abs. 2 Ziff. 1, 186, 52, 59 StGB."

In den Gründen dieses (inzwischen rechtskräftigen) Urteils finden sich keine Ausführungen zum Bundesdatenschutzgesetz.

Fall 8 ("Verkehrsunfall"):

Als sich die A nach dreijährigem Zusammenleben von B trennte, belästigte dieser sie ständig, verklagte sie auf Rückgabe eines Krokodilkoffers, und machte ihr Eifersuchtsszenen. Einmal verfolgte er sie mit seinem Auto, das der Zeuge Z lenkte, als sie ihre Arbeitsstelle verließ. Sie fuhr mit einem Wagen, von dem B wußte, daß er nicht ihr eigener war (den kannte er), sondern ihrem Verlobten V gehörte, von dem B weder Name noch Anschrift wußte. Als es A nicht gelang, den B abzuschütteln, fuhr sie zur Polizei und schilderte die Lage. Diese stoppte den B und unterzog seinen Wagen einer ausgiebigen Verkehrskontrolle, währenddessen A nach Hause fahren konnte. Am nächsten Tag schrieb B an die Zulassungsstelle und bat diese, ihm Auskunft über den Halter des Pkw's zu erteilen, da er gestern abgedrängt und sein Wagen beschädigt worden sei. Er erhielt Auskunft und belästigte nun diesen Halter, nämlich den Verlobten V der A. (Ansprüche wegen des angeblichen Schadens am Auto macht B nie geltend). Als V erfuhr, von wem B die Daten erhalten hatte, stellte er Strafantrag wegen Verletzung des Landesdatenschutzgesetzes. Da Z erst nach Vorführung vernommen werden konnte, verzögerte sich das Verfahren. Knapp ein Jahr nach dem Vorfall, erhob die Staatsanwaltschaft Anklage gegen B: Er habe unbefugt Daten abgerufen und damit gegen § 41 I Ziff. 2 iVm § 11 BDSG verstoßen. Ein halbes Jahr später zog V seinen Strafantrag zurück. Das Amtsgericht stellte daraufhin das Verfahren gemäß § 206 a StPO ein.

Fall 10 ("Jugendstrafe"):

Die auf einem Polizeirevier beschäftigte Sekretärin S, zu deren Tätigkeit auch Abfragen an die Personenauskunftsdatei der Polizei gehörte, lernte im Mai beim Tanz den Betroffenen B kennen, wobei sie nur seinen Vornamen erfuhr. Eine Woche später überraschte sie B dadurch, daß sie ihn mit Nachnamen anredete. Auf seine Frage erklärte sie ihm, daß sie aufgrund des Kennzeichens seines Pkw's seine Personalien auf dem Dienstwege erfahren habe. Einige Wochen später war sie plötzlich sehr einsilbig und zurückhaltend. Auf seine Frage nach dem Grund erklärte sie ihm, daß die über die Datenstation auf dem Revier Angaben über seine Vergangenheit, d. h. Straftat und Haft erhalten habe. Darauf erzählte B ihr seine ganze Lebensgeschichte, einschließlich der zu einer langjährigen (inzwischen verbüßten) Jugendstrafe führenden Straftat. Da auch die Eltern von S eingeweiht wurden, kam es auf deren Drängen zu einer Trennung. Im November desselben Jahres wurde B auf einem Fest von einem Bekannten der B laut gefragt: "Warst Du im Knast?" Als B verneinte, hielt der Bekannte ihm vor, die S, die bei der Polizei arbeitete, sei da anderer Meinung. Als B daraufhin die S telefonisch zur Rede stellen wollte, hängte diese einfach den Höhrer auf. B erstattete daraufhin Strafanzeige wegen Verletzung des Datenschutzgesetzes und stellte Strafantrag. Bei den Ermittlungen stellte sich heraus, daß bei den entsprechenden Zentralcomputern keine Registrierung der von den Dienststellen angeforderten Daten erfolgte, so daß nur Zeugenaussagen als Beweismittel zur Verfügung standen, zumal die Beschuldigte die Aussage verweigerte und eine Durchsuchung ihres Schreibtisches erfolglos blieb. Die Ermächtigung zur Strafverfolgung gem. § 353 II 2 StGB wurde erteilt. Die Staatsanwaltschaft stellte daraufhin das Verfahren gem. § 170 II StPO mit folgender Begründung ein: Die für § 41 BDSG und § 203 StGB erforderlichen Strafanträge seien zu spät gestellt worden, da die Frist bei der Antragstellung im November abgelau-

fen gewesen sei. M habe bereits Ende Mai vom Abruf gewußt. Und weiter wörtlich: "Eine Strafbarkeit wegen Verletzung des Dienstgeheimnisses gem. § 353 b StGB liegt nicht vor. Mitgeteilt hat die Beschuldigte die geheime Tatsache dem Geheimnisträger selbst. Diesem waren aber die mitgeteilten Tatsachen bekannt. Der Anzeigenerstatter hat daraufhin der Beschuldigten seine Lebensgeschichte erzählt, so daß sie als Privat- und nicht als Amtsperson Kenntnis von den Tatsachen erlangt hat und diese aufgrund der Mitteilung auch kein Geheimnis mehr darstellten. Somit entfällt auch hinsichtlich des § 353 b StGB eine Strafbarkeit."

Die Beschwerde des B wurde vom Generalstaatsanwalt verworfen.

Fall 12 ("Hellseherin"):

Als Hellseherin H die Benachrichtigung nach § 34 I BDSG von einer Handelsauskunftei A erhielt, forderte sie von A den Auskunftsbogen an, den sie auch bekam und der folgenden Inhalt hatte:

"Auskunft über H, S-Straße, S-Stadt:

Persönliches	H wurde am x.x.19xx geboren und war von 19xx bis 19xx mit M verheiratet. In der Folge nahm H wieder ihren Mädchennamen an. Die privaten Wohnräumlichkeiten befanden sich in führeren Jahren in der X-Straße in X-Stadt. Von Beruf ist H Hellseherin.
Beurteilung	Die persönliche Beurteilung lautet günstig. Nachteiliges war von keiner Seite zu hören.
Tätigkeit	Wie uns berichtet wurde, ist H als Hellseherin tätig.
Einkommen	Ein Einblick in die Einkommensgrößen ist Außenstehenden nicht möglich.
Grundeigentum	H gilt als Eigentümerin der Eigentumswohnung in der S-Straße in S-Stadt. Eine Grundbucheinsicht war jedoch nicht möglich.
Sonstiges Vermögen	Außer der Wohnungseinrichtung ist kein weiteres Vermögen ersichtlich.
Zahlungsweise	H kam ihren finanziellen Verpflichtungen bisher vereinbarungsgemäß nach. Nachteiliges war von keiner Seite zu hören.

- ohne Vermögensschätzung -"

Auf ihre Beschwerde, daß niemand ein berechtigtes Interesse an ihren Daten gehabt haben könnte, überprüfte A die Angelegenheit und schrieb an H:

... und können Ihnen mitteilen, daß wir die über Ihre Person erteilte Auskunft für nicht existent erklärt und von dem bisher einzigen Auskunftsempfänger zurückgefordert haben."

H wandte sich nun an die Aufsichtsbehörde, die feststellte, daß zwar als Auskunftsgrund "Hausverwaltung" angegeben worden sei, aus diesem allein könne jedoch nicht auf ein berechtigtes Interesse im Sinne von § 32 II BDSG geschlossen werden. Es fehle an dessen glaubhafter Darlegung.

Darauf stellte H Strafantrag. Wenige Wochen später schrieb sie der Staatsanwaltschaft, daß sie durch ihre Begabung auch Hinweise auf bestimmte Personen empfange; sie stellte deshalb Strafantrag gegen B, zumal dieser seine Informationen ihrem geschiedenen Ehemann in die Hände gespielt habe. Außerdem sei bewußt ihr früherer Ehename, den sie abgelegt habe, preisgegeben worden. Als die Polizei von A den Auskunftsbogen anforderte, gab diese an, daß er zum einen sich in ihrer Zentrale in einer anderen Stadt befinde, zum anderen "aufgrund des Bundesdatenschutzgesetzes" sie die Aufzeichnungen auch nicht herausgeben würden. Nachdem sich die A auch gegenüber der Staatsanwaltschaft weigerte, erwirkte diese einen Durchsuchungs- und Beschlagnahmebeschluß für Zentrale und Filiale der A. Der Datenschutzbeauftragte D der A erklärte, daß der Vorgang der Auskunftserteilung nicht unter das BDSG falle, da keine Daten aus einer Datei übermittelt worden seien. Der Staatsanwalt war der Meinung, daß der folgende Auskunfts-"Spiegel", wie er in der "Anleitung für Mitarbeiter der A" als Vorbild abgedruckt war, als Datei im Sinne des BDSG (§ 2 III Nr. 3) anzusehen sei. In der "Anleitung" hieß es unter der Rubrik "Gliederung der Auskünfte über Privatpersonen und freie Berufe":

"Jede Auskunft über Privatpersonen (einschl. freie Berufe, Landwirte) besteht aus:

a) Persönliches
b) Beurteilung
c) Tätigkeit
d) Einkommen
e) Grundeigentum
f) Sonstiges Vermögen
g) Zahlungsweise
h) eventl. Bankverbindung
i) Redaktionszeile
j) Kredit- und Sonderfragenbeantwortung"

Es stellte sich heraus, daß der von H beschuldigte B Datenschutzbeauftragter bei der Firma F war und über diese die Anfrage veranlaßt hatte. Der Anwalt von B erklärte, daß § 41 BDSG ein "eigenhändiges Delikt, welches nicht in mittelbarer Täterschaft begangen werden könne", sei und führte weiter aus: "Ob nämlich die Übermittlung, die Veränderung, der Abruf oder das Beschaffen aus verschlossenen Behältnissen unbefugt ist, ob es sich um personenbezogene Daten handelt, ob diese geschützt und nicht offenkundig sind, ergibt sich erst durch eine überaus komplizierte Verweisungskette innerhalb des BDSG. Es handelt sich also nicht um eine normative Wertung, dieaus dem nebenstrafrechtlichen Tatbestand unmittelbar zu entnehmen wäre, auch nicht um eine in der Laiensphäre nachvollziehbare Wertung, sondern um eine Blankettnorm mit extrem komplizierter und kaum nachvollziehbarer Verweisungstechnik, deren Güterabwägungen methodisch nicht nachvollziehbar sind (Haft NJW 79, 1195)." Und weiter: "Es soll dahingestellt bleiben, daß ein juristischer Laie die bereits erwähnte komplizierte Verweisungstechnik des BDSG nicht nachvollziehen kann. Die notorische "Parallelwertung in der Laiensphäre" ist bei diesem Gesetz platterdings niemanden möglich, wenn daran nach einhelliger Auffassung der Literatur bereits

ausgewachsene Landgerichte "glorreich" scheitern (Haft, NJW 1979, 1195)." Er kommt zum Ergebnis: "Angesichts der feinsinnigen Definitionen und Verweisungsketten des Gesetzes muß nicht nur nach den obigen Ausführungen, die von der herrschenden Meinung allerdings bejahte Frage der Bestimmtheit des Straftatbestandes im Sinne des Art. 103 GG bezweifelt werden."

Die Ermittlungen ergaben weiter, daß der Leiter L der Filiale der A die Prüfung der Frage, ob ein berechtigtes Interesse vorliegt, zu verantworten hatte.

Die Staatsanwaltschaft stellte daraufhin das Verfahren gegen L und B mit Zustimmung des Gerichts nach § 153 a StPO ein.

((Aus der Höhe der Geldauflage in Relation zum Einkommen ergäben sich bei L 30 Tagessätze und bei B 20 Tagessätze.))

Fall 13 ("Betriebsrat"):

Betriebsratsvorsitzender B stellte Strafantrag gegen den Firmeninhaber F, da dieser "Fehlzeitenkarten" der Betriebsratsmitglieder herumgereicht habe, um sie in ihrem Ansehen herabzusetzen und damit gegen Datenschutzbestimmungen verstoßen habe. Die für jedes einzelne Jahr angelegten Karten (in Form einer Karteikarte) enthielten folgende Daten:

> Name, Funktion, Geburtsdatum,
> Firmeneintrittsdatum sowie die
> zustehenden und genommenen Urlaubstage,
> die Fehltage und die Krankheitstage.

Nach ihren Ermittlungen stelle die Staatsanwaltschaft das Verfahren ein:

"Die Karten sind für den innerbetrieblichen Geschäftsablauf bestimmt. Aufgrund dessen bedeutet ihr Vorzeigen innerhalb des Betriebes auch keinen Verstoß gegen § 41 BDSG. Das Verhalten erfüllt auch nicht den Tatbestand des § 119 I Ziff. 3 BetrVG ..., da ... die allgemeine Anerkennung und Wertschätzung durch Kollegen ... nicht erfaßt wird."

B legte Beschwerde ein und begründete sie damit, daß es sich hier um vertrauliche Personalunterlagen handele und die Bekanntgabe in betriebsfremden Räumen erfolgt sei. Die wiederaufgenommenen Ermittlungen verzögerten sich, da inzwischen auch (weitere) Behinderungen des Betriebsrates (u. a. das Öffnen von Briefen) gerügt wurden. In der Zwischenzeit schied B aus der Firma aus und F fiel in Konkurs. Das Verfahren wurde dann bezüglich der Behinderung des Betriebsrates (§ 119 BetrVG) wegen verspäteten Strafantrages eingestellt. Weiterer hinreichender Tatverdacht liege nicht vor.

Fall 15 ("Nachbarsjunge"):

Die 52jährige ledige Angestellte A erhielt eine Anstellung bei der Kriminalaktenhaltung der Kriminalpolizei in Niedersachsen. Unmittelbar nach Arbeitsaufnahme sah sie aus reiner Neugierde nach, ob über den im selben Hause wohnenden 16jährigen Nachbarsjungen N eine Kriminalakte angelegt war. Dazu brauchte sie nur an ihrem Arbeitsplatz eine entsprechende Indexkarte zu ziehen und so die Aktennummer feststellen und dann die Akte zur Hand zu nehmen.

Als N, der im Alter von 11 Jahren einen Ladendiebstahl begangen hatte, ein polizeiliches Führungszeugnis benötigte, erinnerte sich seine Mutter daran, daß die Mutter der A beiläufig gesagt hatte, daß über N bei der Kripo eine Akte bestünde. Da die Mutter des N nunmehr befürchtete, N werde kein Führungszeugnis ohne Eintragungen bekommen, rief sie bei der Polizei an, um sich zu erkundigen, worauf die Ermittlungen gegen A begannen. Bei der Vernehmung der Eltern des N gaben diese an, daß sie sich nicht geschädigt fühlten und ausdrücklich auf die Stellung eines Strafantrages verzichteten. Der Vorgang wurde daraufhin dem niedersächsischen Landeskriminalamt (LKA) zur Stellungnahme gesandt, das der Meinung war, auch der "Herr der Daten" sei Betroffener und damit strafantragsberechtigt nach § 21 NDSG. Da aber sowohl die Aktensammlung als auch die genutzte Indexkarte in der ausschließlichen Verfügungsgewalt der Kripo stehe, sei sie und nicht der Direktor des LKA "Herr der Daten". Allerdings sei notwendig, daß eine Datei, gleichgültig, ob sie im konventionellen oder automatisierten Verfahren bearbeitet werde, vorliege. Die Aktenindexkartei sei zwar eine Datei, tatsächlich sei aber die Auskunft aus der Aktensammlung (die keine Datei sei) erteilt worden, was aber wiederum nur über die Indexkartei möglich gewesen sei. "Inwieweit diese Handlungsabfolge einen Verstoß gegen das NDSG darstelle, müßte im richterlichen Ermittlungsverfahren entschieden werden."

Nachdem der Leiter der Kripo daraufhin Strafantrag gestellt hatte und die Ermächtigung nach § 353 d III StGB eingeholt worden war, wurde die Akte der Staatsanwaltschaft übersandt, die der Meinung war, daß für eine Bestrafung nach § 353 b StGB die Gefährdung wichtiger öffentlicher Interessen, bezüglich § 203 StGB ein Strafantrag fehle. "Eine strafbare Handlung nach dem NDSG liegt nicht vor. Gemäß § 1 Abs. 2 Satz 2 NDSG ist die Strafvorschrift des § 21 NDSG nicht anwendbar, weil der Index für die Kriminalakten nicht für Dritte bestimmt ist und in einem nichtautomatisierten Verfahren erstellt wird. Die Kriminalakten selbst fallen nicht unter das NDSG."

Das Verfahren wurde deshalb nach Anhörung von Polizei und Ministerium (vgl. Nr. 90 RiStBV) eingestellt.

Fall 19 ("Roulettspieler"):

Roulettspieler R stellte über seinen Rechtsanwalt im Oktober Strafantrag gegen die Spielbank S (1) wegen unbefugter Übermittlung personenbezogener Daten gemäß § 41 BDSG. Er habe im August mit Erfolg dort Roulett gespielt und während einer Gewinnserie sei ihm eröffnet worden, daß er für die Spielbank S (1) gesperrt werde. Als er einige Zeit später die Spielbank S (2) in einer anderen Stadt aufgesucht habe (und dort verloren habe), sei ihm auch dort eine Sperre erteilt worden. Die sich herausgestellt habe, sei eine Mitteilung von S (1) an S (2), zwischen denen keinerlei rechtliche Verbindung bestehe, der Grund gewesen.

Bei den Ermittlungen fand sich bei S (1) folgendes Schreiben einer dritten Spielbank S (3):

"Sehr geehrte Herren!

Folgende unten namentlich aufgeführte Personen, die Ihre Spielbank besucht haben können,wurden uns als vermutlich einer internationalen Berufsspielerorganisation angehörig gemeldet."

Es folgten (in willkürlicher Reihenfolge) knapp 20 Namen, die (immer in derselben Weise) folgende Angaben enthielten:

Name, Vorname,
Geburtsdatum und -ort (-land),
Nationalität,
Wohnort (teilweise auch noch Straße).

Auch die entsprechenden Angaben über R befanden sich darunter. Daraus wurde von S (1) eine alphabetisch geordnete Liste mit diesen Daten hergestellt.

Bei den Ermittlungen behaupteten die Verantwortlichen von S (1), sie hätten von einem Mitarbeiter der Spielbank S (4) den Hinweis auf den Sperrvermerk und nicht von S (1) erhalten. Aufgrund dessen stellte die StA das Verfahren ein: "Den bei der Spielbank S (1) angestellten Beschuldigten ist ein Verstoß gegen das Datenschutzgesetz nicht nachzuweisen."

Nach der vom Rechtsanwalt des R eingelegten Beschwerde entschied der Generalstaatsanwalt: "Ob das Bundesdatenschutzgesetz auf den vorliegenden Fall anwendbar ist, kann auf sich beruhen, weil die Tat jedenfalls nicht beweisbar ist."

Darauf stellte der Anwalt einen ausführlich begründeten Antrag auf gerichtliche Entscheidung nach § 172 II StPO. Das OLG verwarf jedoch den Antrag als unzulässig, "weil er nicht den Anforderungen des § 172 II StPO genügt, da es an einer Auseinandersetzung mit den Gründen der Bescheide der Staatsanwaltschaft fehlt."

Fall 20 ("Bibliotheksbenutzerausweis"):

Bibliotheksbenutzer B gab ein Buch nicht rechtzeitig zurück und bekam eine Mahnung zugesandt. Dies geschah in der Weise, daß der, mit ca. 3 000 anderen, auf Mikrofilm gespeicherte Benutzerausweis fotokopiert wurde und dann so in ein Fensterkuvert eingelegt wurde, daß nur Name und Anschrift sichtbar waren. Bei B nun war im Fensterkuvert das links neben der Postleitzahl stehende Geburtsdatum und die unterhalb des Ortes befindliche Unterschrift sichtbar. Er forderte daraufhin einen neuen Benutzerausweis, die Vernichtung des Mikrofilms und legte Dienstaufsichtsbeschwerde ein. Da ihm die Antwort des Bibliotheksdirektors nicht zu genügen schien, stellte er Strafantrag.

Der als Beschuldigte vernommene Direktor D führte aus, daß bisher noch nie Beschwerden gleicher Art vorgekommen seien, dennoch aber aufgrund dieses Falles eine neue Arbeitsanweisung für das Ausstellen von Benutzerausweisen ergangen sei, um solche Vorkommnisse zu verhindern. Im übrigen habe die Aufsichtsbehörde auf Anfrage erklärt, daß Mikrofilme keine Dateien seien. Außerdem seien die Daten nicht zur Übermittlung an Dritte bestimmt und wurden "nicht zu automatisierten Verfahren verarbeitet".

Die Staatsanwaltschaft beauftragte daraufhin die Polizei, sich den Vorgang einer Ausleihe und Versendung von Mahnschreiben von der Bibliothek vorführen, sowie Vergleichs- bzw. Demonstrationsmaterial herstellen zu lassen. Das Verfahren wurde danach gemäß § 170 II StPO eingestellt: Zum einen sei die konkret handelnde Person nicht zu ermitteln gewesen, zum anderen handele es sich bei der unkorrekten Versendung offensichtlich um ein Versehen, also fahrlässiges Verhalten. Nach dem Landesdatenschutzgesetz sei aber nur vorsätzliches Handeln strafbar.

B legte daraufhin Beschwerde mit der Begründung ein, auch fahrlässiges Handeln sei strafbar. In einem Vermerk legte die Staatsanwaltschaft dar, daß nur vorsätzliches Handeln strafbar sei und führte weiter aus:

"Auf die zweifelhafte Frage, ob es sich bei den bei der Fotoverbuchung entstehenden Mikrofilme, von denen durch Ablichtung die Mahnschreiben gewonnen werden, überhaupt um Dateien im Sinne des Landesdatenschutzgesetzes handelt, kommt es nach dem oben gesagten nicht entscheidend an." Der Generalstaatsanwalt wies die Beschwerde zurück, da nur vorsätzliches Handeln strafbar sei, dieses aber nicht nachzuweisen gewesen sei.

Danach beantragte der RA des B eine gerichtliche Entscheidung nach § 172 II StPO und begründete dies in einem 12seitigen Schriftsatz ausführlich, wobei er sich auch mit dem Inhalt der Bescheide der Staatsanwaltschaft auseinandersetze. Der Generalstaatsanwalt beantragte die Verwerfung als unzulässig - hilfsweise als unbegründet - und führte aus:"M. E. entspricht der Klagerzwingungsantrag nicht der in § 173 III 1 StPO vorgeschriebenen Form, weil der Gang der Ermittlungen nur unvollständig geschildert worden ist und hinsichtlich des Beschuldigten D Tatzeit und Beweismittel nicht angegeben worden sind." ... "Die Fotoverbuchung stellt keine Datei dar." Außerdem bestehe kein hinreichender Verdacht für vorsätzliches Handeln. Das OLG verwarf daraufhin den Antrag des B als unzulässig: "Der Gang des Ermittlungsverfahrens wird in dem Antrag nicht ausreichend geschildert."

Fall 21 ("Mikrofichesfund"):

Der selbständige Bankkaufmann B kaufte im Oktober 1977 von der V-Bank gebrauchte Schreibtische. Beim Säubern entdeckte er neben Überweisungen und Tagesauszügen etwa 40 bis 50 Mikrofiches (im COM-Verfahren hergestellt) mit je ca. 2 000 Kundenadressen, die der A-Bank (Muttergesellschaft der V-Bank) gehörten und beim Verkauf vergessen worden waren. Zusammen mit seinem (damaligen) Teilhaber T schnitt er die an den Rändern befindliche Aufschrift "A-Bank" ab und sie versuchten die Mikrofiches, deren Wert (pro Adresse zwischen 0,10 und 1,00 DM) sie erkannten, für eigene Zwecke zu verwerten. Die Mikrofiches enthielten - nach Namen geordnet - neben Anschrift, Geburtsdatum, Kontonummer und Kreditmodalitäten einschließlich eventl. Bürgen, noch weitere Daten.

Die Verwertung gelang nicht im erwarteten Umfang, da von 1 000 angeschriebenen Personen nur zwei antworteten und auch mit ihnen kein Finanzierungsgeschäft zustandekam. Deshalb verkauften sie dem befreundeten Finanzierungsmakler F, nachdem sie ihm die Herkunft erzählt hatten, 20 Mikrofiches für insgesamt 5 000 DM. Aber auch F, der wiederum T in die Verwertung eingeschaltet hatte, gelang keine zufriedenstellende Auswertung. So beschlossen F und T unter Einschaltung eines befreundeten Vertreters V an den Zeugen Z, dem sie gegenüber andeuteten, daß "die Sache nicht ganz sauber" sei, 15 Mikrofiches für schließlich 10 000 DM zu verkaufen. Z ging zum Schein darauf ein, verständigte die Polizei und bei der Übergabe wurden T und V festgenommen.

Nach Abschluß der Ermittlungen legte der Staatsanwalt in einem Vermerk dar, daß es fraglich erscheine, ob B die personenbezogenden Daten an F "übermittelt" habe: "Zweifellos ist F Dritter. Nicht jede Form der Bekanntgabe ist jedoch ein "Übermitteln". Im Hinblick auf § 1 Abs. 2 Satz 1 BDSG müssen vielmehr in Dateien gespeicherte Daten übermittelt werden. Da die Daten die B (bzw. T) nicht mehr in einer Datei gespeichert waren, ist die Weitergabe durch ihn kein Übermitteln in Sinne der Vorschrift. Eine etwa noch bestehende Speicherung bei der A-Bank ist bedeutungslos (vgl. Ordemann/Schomerus § 2 BDSG 2.2). Es fehlt damit auch an der Weitergabe der Daten durch eine datenverarbeitende Stelle." Die Frage der Strafantragsberechtigung der A-Bank könne offen bleiben.

Es wurden gegen B, T, F und V antragsgemäß Strafbefehle in Höhe von jeweils 50 Tagessätzen erlassen: Bei B und T wegen Unterschlagung, bei F und V wegen Hehlerei. Nur B bezahlte, während die anderen Einspruch einlegten. Als die Hauptverhandlung ausgesetzt wurde, legte der nunmehr mit der Sache befaßte Staatsanwalt in einem Vermerk dar:

"Entgegen dem Vermerk ... haben die Angeklagten sich m. E. auch wegen eines Vergehens gegen das Bundesdatenschutzgesetz strafbar gemacht (§ 41 Abs. 1 Nr. 2 und Abs. 2 BDSG). Sie haben nämlich gespeicherte Daten weitergegeben, wobei sie auch "speichernde Stelle" i. S. d. § 2 Abs. 2 Nr. 2 BDSG waren. Speichern i. S. d. § 2 BDSG ist nämlich auch das bloße Aufbewahren von Daten zum Zwecke ihrer weiteren Verwendung. Dies lag hier vor, weil jede einzelne Mikrofilmkarte bereits als Datei i. S. d. § 2 BDSG zu behandeln ist und die im vorliegenden Fall sichergestellten Karten aufbewahrt worden waren, um sie zunächst selbst auszuwerten bzw. später zum eigenen Vorteil an andere abzugeben."

Er veranlaßte, daß bei einem der betroffenen Kunden (K) nachgefragt wurde, ob er Strafantrag stellen wolle, was K auch tat.

In der anschließend stattfindenden Hauptverhandlung erging gegenüber T und V ein rechtlicher Hinweis in Bezug auf § 41 BDSG, gegen F wurde Nachtragsanklage erhoben.

Das Gericht verurteilte T wegen Unterschlagung, F und V wegen Hehlerei zu einer Geldstrafe in Höhe von jeweils 50 Tagessätzen. In den Gründen stellte das Gericht u. a. fest:

"Vergehen des Verstoßes gegen das Datenschutzgesetz lagen nicht vor. Ein Übermitteln im Sinne von § 41 BDSG war nicht zu bejahen. Übermitteln ist das Bekanntgeben von Daten in der Weise, daß die Daten durch die speichernde Stelle weitergegeben oder zur Einsichtnahme, namentlich zum Abruf, bereit gehalten werden. Voraussetzung danach ist somit, daß die Vermittlung von der speichernden Stelle ausgeht. Speichernde Stelle war hier unzweifelhaft die Zweigstelle der A-Bank. Nicht aber war speichernde Stelle der Angeklagte F, von dem aus sie zuletzt an den Zeugen Z gehen sollten. Unabhängig von dem Bedenken, ob auch speichernde Stelle derjenige sein kann, der durch eine Vermögensstraftat an die Daten gelangt ist, war der Angeklagte F keine speichernde Stelle mehr. Speichernde Stelle gemäß § 2 Abs. 3 Nr. 1 BDSG sind Personen oder Stellen, die Daten für sich selbst speichern bzw. oder durch Andere speichern lassen. Dies traf bei dem Angeklagten F nicht zu. Der Angeklagte F hatte überhaupt keinen Verwendungszweck mehr, als er die Mikrofilmkarten, wie er es sagt, doch noch zu Geld machen wollte, um die Auslagen herauszubekommen. So war ein Verwendungszweck im Sinn- des § 2 Abs. 2 Nr. 1 BDSG nicht vorhanden gewesen. Auch fehlt es bei der gegebenen Sachlage am Übermitteln im Sinne des § 41 BDSG in Verbindung mit § 2 Abs. 2 Nr. 2 BDSG. Zum Übermitteln gehört die Weitergabe oder das Bereithalten zur Einsichtnahme, wie die Legaldefinition des BDSG ergibt. Diese Weitergabe muß aber insoweit erfolgt sein, daß der Dritte, an den übergeben worden ist, mit den Daten auch etwas anfangen und arbeiten kann. Dies war hier nicht der Fall, zumindest nicht feststellbar. Bei der Feststellung, ob ein Verstoß gegen das BDSG vorliegt, war von dem Strafantragsteller auszugehen. Es ging darum, ob die Daten des K weitergegeben worden waren im Sinne des § 2 Abs. 2 Nr. 2 BDSG. Dies war hier auf der einen Seite im tatsächlichen Bereich nicht festzustellen, da nicht festzustellen war, ob nun ausgerechnet die Daten des K bereits in der Weise übergeben worden waren, daß der Zeuge Z damit hätte arbeiten können. Im übrigen war hier bezüglich des Merkmals zu übermitteln noch festzustellen gewesen, daß gerade bei dem Vorgang der Übergabe die Polizei hinzukam, so daß auch von da aus gesehen die Übermittlung erst im Versuchsstadium gewesen ist, als die Polizei eingriff, ein Versuch aber gemäß § 41 BDSG nicht strafbar ist.

Nach alledem waren weder der Angeklagte F noch der Angeklagte V eines Vergehens gegen das BDSG überführt."

Da alle drei Angeklagten Berufung einlegten, kam es erneut zur Verhandlung, allerdings wurde nur die Höhe und nicht die Anzahl der Tagessätze geändert. Ausführungen zum BDSG enthielt das Berufungsurteil keine.

F und V legten Revision ein, die F zurücknahm. Anfang 1984 stand ein Revisionstermin für V noch aus.

Fall 23 ("Kreditangebote"):

Die B-Bank ließ ihre Daten im Rechenzentrum R verarbeiten. Dort wurden Mikrofiches hergestellt, die mehrmals täglich vom und zum Rechenzentrum transportiert wurden, wobei der Verteiler ca. 20 Stellen umfaßte. Auf den Mikrofiches wurden für jedes Giro-, Spar- oder sonstiges Konto, folgende Daten gespeichert:

Name, Straße, Postleitzahl, Ort, Geburtsdatum, Konto-Nummer, Saldo, Zahlstand, NFR-Rate und Mahnstand.

Die Mikrofiches waren alphabetisch nach Namen geordnet und das Umsortieren oder Aussortieren,z. B. nach Postleitzahlbezirken,war möglich.

Als die B-Bank erfuhr, daß eine G-GmbH Werbesendungen ("günstige Kredite") an ihre Kunden versandte (mit den gleichen Erfassungsfehlern in den Adressen wie bei ihr), ermittelte sie, daß die G-GmbH, zum Preis von 0,15 DM pro Stück, Adressen gemietet hatte, (teilweise angeblich von einer Schweizer Firma F) und davon ca. 20 000 Adressen von ihr stammen könnten. B stellte darauf Strafanzeige gegen Unbekannt wegen Diebstahl und fünf Wochen später wegen Verstoßes gegen § 41 BDSG. Sie berichtete der Staatsanwaltschaft weiter, daß sie erfahren habe, daß der Geschäftsführer der G-GmbH vor zwei Jahren dem Überbringer eines EDV-Bandes der B-Bank 50 000 DM gezahlt haben soll. Desweiteren nannte B sieben Firmen, die angeblich auch (Teile) ihres Adressenmaterials gekauft und verarbeitet haben sollen. Die Ermittlungen bei der Druckerei,über die die Werbeschreiben versandt wurden, ergab, daß sowohl Mikrofiches als auch ein EDV-Band mit Adressen geliefert worden waren. Es stellte sich nun auch heraus, daß die Inhaber I einer Versicherungs- und Finanzierungsfirma, die mit der B-Bank zusammenarbeitete, in einer anderen Stadt Strafantrag wegen Verletzung von § 17 UWG und § 41 BDSG gestellt hatte, nachdem sie die Werbebriefe erhalten hatte. Inzwischen tauchten auch Werbeschreiben einer schweizerischen Bank S, der Verbindungen zur G-GmbH nachgesagt wurden, auf und die B-Bank ließ über Dritte einen als Probe angebotenen Mikrofiches zum Preis von 1 000 DM kaufen. Es stellte sich heraus, daß es sich "um einen direkt von einem der 12 Original-Micro-Fiche erstellten Duplikat-Micro-Fiche auf Vesikular-Material und nicht um ein Duplikat eines Duplikat-Micro-Fiches" handelte. Eine Durchsuchung der Räume der G-GmbH, bei der auch EDV-Fachleute der B-Bank zugezogen waren, blieb erfolglos.

Da auch weitere umfangreiche Ermittlungen erfolglos blieben, wurde das Verfahren eingestellt.

Fall 24 ("Mitgliederabwerbung"):

Eine Allgemeine Ortskrankenkasse (AOK) erstattete Strafanzeige gemäß § 203 II StGB und § 41 BDSG gegen Unbekannt: Ein privates Krankenversicherungsunternehmen K betreibe eine intensive Mitgliederwerbung gegenüber bestimmten ihrer Angestellten. Da K wisse, daß es sich bei diesen Angestellten um nur freiwillig bei der AOK versicherten Mitarbeiter handele und zudem noch deren Geburtsdatum kenne, sei zu vermuten, daß die Informationen von anderen Mitarbeitern weitergegeben worden seien. Hausinterne Ermittlungen seien erfolglos geblieben. Die Daten würden in einer EDV-Anlage verarbeitet, auf Magnetbändern gespeichert und dann mikroverfilmt, wobei in jeweils mehrfachen Ausfertigungen drei Arten (mit jeweils anderen Ordnungskriterien) von Mikrofiches hergestellt würden. Daneben existierten, in Form von Computerausdrucken,

Beitragsbücher und manuell geführte Karteikarten. Der besondere Status der angesprochenen Angestellten sei aus allen "Quellen" ersichtlich. Einsichtsberechtigt seien etwa 200 Sachbearbeiter.

Da bei den Ermittlungen der Staatsanwaltschaft zudem bekannt wurde, daß K angeblich bestimmten AOK-Angestellten Provisionen in Aussicht gestellt hatte, wurden die Räume der K durchsucht. Zwar fanden sich Karteikarten mit Adressen und Status von AOK-Angestellten, K gab jedoch an, diese seien von anderen Kunden und Interessenten mitgeteilt worden. Ferner schrieb der Anwalt der K, daß von den Betroffenen kein Strafantrag vorliege. "Der Antrag wurde vielmehr vom Geschäftsführer der AOK als speichernder Stelle der personenbezogenen Daten gestellt. Da er nicht Betroffener im Sinne des BDSG ist, besteht für ihn kein Antragsrecht." Abgesehen davon, wäre eine Übermittlung nach § 24 II BDSG zulässig. Darauf schrieb der Staatsanwalt an den Geschäftsführer der AOK, daß das Verfahren eingestellt worden sei, da der erforderliche Antrag von den Verletzten nicht gestellt worden sei. "Der von Ihnen gestellte Strafantrag erfüllt nicht die Voraussetzungen der §§ 203 StGB und 41 Abs. 3 Bundesdatenschutzgesetz, da hier allein antragsberechtigt die Geschädigten sind, deren Privatgeheimnisse weitergegeben wurden, und nicht auch der Anvertraute, also der AOK."

Fall 25 ("Mikroficheeinsicht"):

Der ehemals beim Arbeitsamt beschäftigte Heranwachsende H schlich sich knapp drei Wochen nach dem ihm dort gekündigt worden war, nach Ende der Dienstzeit durch den Personaleingang ein. Er entwendete aus der Schublade eines Schreibtisches einen Schlüssel für einen Stahlschrank, öffnete diesen und entnahm ihm einen Mikrofiche, auf dem Leistungsdaten abgelichtet waren. Dann schob er ihn in das im Zimmer stehende Datensichtgerät, um Einsicht zu nehmen. Als er von einem Angestellten überrascht wurde, gab er an, daß er bezüglich seines eigenen Leistungsfalles keine Auskunft bekommen hätte und da seine Mutter den Antrag abgegeben habe, wolle er wissen, ob dieser bewilligt sei. Der Direktor des Arbeitsamtes stellte zunächst Strafantrag wegen Hausfriedensbruch und später "gem. § 41 BDSG".

Es wurde ein Strafbefehl gegen H erlassen, indem ihm neben einem Vergehen des § 123 StGB vorgeworfen wurde, daß er gegen das Bundesgesetz über den Datenschutz verstoßen habe: "Sie haben nicht offenkundige Daten aus Ihren Leistungsakten über ein Datensichtgerät eingesehen." Strafantrag sei gestellt worden vom Direktor des Arbeitsamtes bezüglich § 123 StGB (sofort) und § 41 BDSG (später). Das Gericht erließ den Strafbefehl mit einer Geldstrafe in Höhe von 15 Tagessätzen.

Fall 26 ("Zeitungsabonnenten"):

Die Datenverarbeitungsservice-GmbH D hatte in ihrer Anlage insgesamt 100 000 Adressen, darunter u. a. die Abonnenten der Z-Zeitung gespeichert. Eines Tages wurde dem Geschäftsführer G der D von K,einem Konkurrenzunternehmen der Z-Zeitung mitgeteilt, daß sie eben telefonisch von einem Unbekannten Computerlisten mit Zeitungsabonnenten der Z-Zeitung angeboten bekommen hätten und daß dieser als Beweis eine solche Liste schicken werde. G verständigte daraufhin die Polizei. Er war sich sicher, daß keine Magnetbänder gestohlen worden waren und angesichts der Datensicherungsmaßnahmen nur einer von fünf bestimmten Mitarbeitern die Computerausdrucke gestohlen haben konnte. Als die Ausdrucke bei K eintrafen, konnte festgestellt werden, daß es tatsächlich Ausdrucke der D-GmbH waren. Es handelte sich dabei um ordnungsgemäß und auf Weisung hergestellte Kontrollausdrucke, die eigentlich in einen besonderen Abfallbehälter hätten abgelegt werden müssen. Da der Umschlag mit dem Ausdruck in der Stadt S abgesandt worden war und dort die führere Freundin F des Programmierers P wohnte, und zudem anscheinend andere Indizien vorlagen (P hatte während seiner fast zweijährigen Beschäftigungszeit häufiger gemaßregelt werden müssen, zu vernichtende Ausdrucke nicht einfach in einen Papierkorb zu werfen), vermutete G, daß P der Täter sein könnte. "Vorsorglich stelle er Strafantrag für alle Fälle". Darauf wurde der Vorgang der Staatsanwaltschaft übergeben.

Der von ihr wegen Verdachts von Straftaten nach §§ 5, 41 BDSG, § 17 UWG und § 246 StGB beantragte Durchsuchungsbefehl gegen F und P führte zu keinem Erfolg. Die Vernehmung der F ergab die alleinige Ausführung der Handlung durch P. Darauf wurde von der Staatsanwaltschaft Anklage vor dem Schöffengericht wegen §§ 242, 248a, 53 StGB, 1 ff., 41 BDSG (nicht wegen § 17 UWG, denn "bei der Liste handelt es sich nicht um ein Betriebsgeheimnis im Sinne von § 17 UWG") erhoben. P war in der Verhandlung geständig, den Kontrollausdruck an sich genommen und weitergeleitet zu haben. Im übrigen wurde festgestellt, daß für die D-GmbH Strafantrag gestellt worden sei, und es erging der rechtliche Hinweis, daß auch eine Verurteilung nach § 41 II BDSG in Betracht kommen könnte. Die Staatsanwaltschaft beantragte für P (der wegen anderer Delikte vorbestraft war) drei Monate Freiheitsstrafe mit Bewährung. Der Tenor des Urteils lautete:

> "Der Angeklagte wird wegen unbefugter Übermittlung von nach dem Bundesdatenschutzgesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, in Tateinheit mit Diebstahl einer geringwertigen Sache zu einer Freiheitsstrafe von vier Monaten verurteilt, deren Vollstreckung zur Bewährung ausgesetzt wird. (§§ 41 I Bundesdatenschutzgesetz, 242, 248a, 52, 56 StGB)."

Daß P auch Bereicherungsabsicht gehabt habe (§ 41 II BDSG), glaubte das Gericht nicht mit der erforderlichen Sicherheit feststellen zu können. P legte Berufung ein, die jedoch, da er nicht zur Verhandlung erschienen war, gemäß § 329 StPO verworfen wurde.

Fall 27 ("Multifunktionär"):

Kanzler K der Universität U versandte vor einer entsprechenden Gremiensitzung ein Rundschreiben an die Dekane und Mitglieder der Universitätsgremien, um sie auf das in seinen Augen außerhalb der rechtmäßigen Aufgabenerfüllung liegende Verhalten des Rektors R hinzuweisen. Hierin hielt er R unter anderem vor, daß er einen sich bereits im 11. Semester seines Zweitstudiums befindlichen Studenten und "Multifunktionär" M, der zudem noch keine Zwischenprüfung abgelegt habe, zum nebenberuflichen Studienberater eingesetzt habe. M stelle daraufhin über seinen Rechtsanwalt Strafantrag wegen Verstoßes gegen § 41 BDSG und benachrichtigte den Landesdatenschutzbeauftragten. Der als Beschuldigte vernommene K erklärte, daß er die Angaben über M aus dessen Akte, die er während eines Antrages des M zu bearbeiten gehabt habe, entnommen habe. Außerdem sei dieÜbermittlung zur rechtmäßigen Aufgabenerfüllung erforderlich gewesen und zudem sei die Übermittlung nicht an Dritte im Sinne des Landesdatenschutzgesetzes erfolgt. Die Staatsanwaltschaft stellte das Verfahren nach § 170 II StPO ein: K habe sich nicht eines Vergehens nach dem Landesdatenschutzgesetz strafbar gemacht (das BDSG finde keine Anwendung), da er die Daten aus studentischen Akten, die er zudem aufgrund seiner Befugnis jederzeit einsehen dürfe, entnommen habe. Und weiter wörtlich: "Ein automatisiertes Verfahren gibt es im Zusammenhang mit diesen Akten nicht. Selbst wenn dieselben Daten des Anzeigenerstatters (M) zusätzlich noch in einer Datei im Sinne des Landesdatenschutzgesetzes gespeichert sein sollten, läge ein strafbares Verhalten des Beschuldigten nicht vor, weil ein Übermitteln oder Abrufen nicht erfolgte. Beides setzt nämlich eine Datei als Quelle voraus."

Die Beschwerde des M wurde vom Generalstaatsanwalt verworfen.

Fall 32 ("Bankindiskretion"):

Lagerarbeiter L zog aufs Dorf und fand dort Arbeit. Als er sein Girokonto überzog, sprach das Vorstandsmitglied V der Bank beim Arbeitgeber des L vor und teilte ihm in diesem Zusammenhang mit, daß sich aufgrund von Nachforschungen ergeben habe, daß L zweimal die eidesstattliche Versicherung abgegeben habe und in diesem Verfahren Haftbefehl erlassen worden sei. Als L gekündigt wurde, stellte er Strafantrag wegen Verstosses gegen das Datenschutzgesetz. Nach kanpp vier Wochen stellte die Staatsanwaltschaft das Verfahren ein, da sich keine Anhaltspunkte für einen Verstoß gegen das Datenschutzgesetz ergeben hätten. Auf die Beschwerde des L wies der Generalstaatsanwalt die Staatsanwaltschaft an, das Verfahren wieder aufzunehmen, da der Verdacht eines Vergehens nach § 41 I Nr. 1 BDSG bestünde. Nach weiteren Ermittlungen wurde schließlich ein halbes Jahr später Anklage erhoben: V habe unbefugt personenbezogene Daten, die nicht offenkundig seien, übermittelt. Das Gericht lehnte jedoch die Eröffnung des Hauptverfahrens ab: "Das Hauptverfahren kann nicht eröffnet werden, da es an einem hinreichenden Tatverdacht fehlt (§§ 203, 204 StPO). Denn die Amtsgerichte können jedermann auf Anfrage Auskunft über das Vorliegen von eidesstattlichen Versicherungen und Haftbefehlen bezüglich einer Person Auskunft erteilen. Die im vorliegenden Fall übermittelten Daten waren daher offenkundig. Bei Durchführung einer Hauptverhandlung müßte der Angeschuldigte daher freigesprochen werden."

Fall 34 ("Studienfachangabe"):

Student S stellte Strafantrag gegen den Universitätspräsidenten wegen Verdachts des Verstoßes gegen das Datenschutzgesetz. Bei ihm sei der Mitarbeiter der G-GmbH erschienen und habe ihn um die Beantwortung persönlicher Fragen gebeten, da die Universität mit der G-GmbH zusammen Umfragen durchführe und er als Proband ausgewählt worden sei. Der Mitarbeiter habe zudem die gleichen Adressenaufkleber wie sie die Universität für amtliche Schreiben verwenden würde, verwandt.

Bei den Ermittlungen stellte sich heraus, daß die G-GmbH ein von Bund und Ländern als Gesellschaftern getragenes gemeinnütziges Planungsunternehmen für Fragen des Hochschulbereichs ist, das ein Gutachten über Maßnahmen zur Anpassung der Personalstruktur an das Hochschulrahmengesetz erstatten sollte. Die Uni erklärte, daß das Einverständnis der Studenten vorgelegen habe, da nur unter denen, die sich auf dem Fragebogen bei der Immatrikulation bereit erklärt hätten, daß ihre Anschrift in einem öffentlichen Adressbuch der Uni erscheint, die Probanden ausgesucht worden wären. Beim Anzeigenerstatter S sei dies zwar nicht der Fall gewesen, da er die entsprechende Frage verneint habe, durch ein bedauerliches Versehen, das nicht mehr klärbar sei, sei jedoch in der EDV-Anlage bei den Stammdaten ein positives Merkmal gespeichert gewesen. Übermittelt worden seien folgende Daten:

Studienfach,
angestrebte Abschlußprüfung,
Fachsemester,
Familienname, Vorname,
Heimatanschrift,
Semesteranschrift.

Daraufhin fand sich in den Akten der Staatsanwaltschaft folgender Vermerk:

"Die Strafnorm des Landesdatenschutzgesetzes ist objektiv erfüllt. Auch wenn S der Veröffentlichung seiner Anschrift im Adressbuch der Uni zugestimmt hätte, wovon seitens der Uni ohne Verschulden ausgegangen werden durfte, so hätte diese Zustimmung nur die Weitergabe der Semesteranschrift und der privaten Telefonnummer gedeckt, keinesfalls aber die Weitergabe der angestrebten Abschlußprüfung, des Studienfachs und der Fachsemesterzahl an die G-GmbH.

Der nun als Beschuldigte vernommene Abteilungsleiter A der Uni rechtfertigte sein Tun damit, daß das Projekt unzweifelhaft in die Aufgabenstellung der Hochschule gehöre und bemerkte weiter, daß "die Angabe des Studienfaches bei dem einzelnen Studenten als letztlich öffentlich bekanntes Merkmal anzusehen" sei. Die Staatsanwaltschaft stellte daraufhin das Verfahren mit folgender Begründung ein: Zunächst liege kein Übermitteln im Sinne der Legaldefinition vor, da die G-GmbH im Verhältnis zur Uni nicht "Dritter" im Sinne des Gesetzes sei, da sie von der Uni beauftragt worden sei. Ferner sei sie eine "sonstige öffentliche Stelle" im Sinne der Vorschrift des Landesdatenschutzgesetzes über die Datenübermittlung innerhalb des öffentlichen Bereichs. Zum Schluß fehle es an den subjektiven Voraussetzungen, da A von einer Zustimmung des S ausgegangen sei.

Fall 35 ("Viehstatistik"):

Landwirtin L betrieb mit ihrem Ehemann im Außenbereich einer kleinen Gemeinde einen landwirtschaftlichen Nebenerwerbsbetrieb mit einer Schweinemast. Für einen dazu geplanten Erweiterungsbau versagte die Gemeinde die Zustimmung, weswegen L dagegen vor dem Verwaltungsgericht klagte. In der Klagerwiderung der Gemeinde führte diese als Versagungsgrund an, daß "nur ca. 40 Schweine" gehalten würden. Da aber der Bestand bei L zwischen 25 und 100 Tieren schwankte und bei der Erhebung des Tierseuchenbeitrags durch die Gemeinde der Bestand gerade bei 43 Schweinen lag, beschuldigte L den Bürgermeister B, er habe die Daten der Viehzählung (die auch in einer EDV-Anlage der Verbandsgemeindeverwaltung gespeichert waren) unter Verstoß gegen das Datenschutz- und Statistikgesetz mißbräuchlich benutzt. Da im übrigen 80 Liegeplätze vorhanden seien und die Stallungen von niemand betreten werden dürften, könne die Gemeinde nur so auf "ca. 40" kommen. Sie führte weiter aus: "Hier sind es die Schweine, und was geschieht mit den anderen Daten? Muß bei den Bäuerlein alles gezahlt werden? Ist das nicht ein bißchen zuviel Staat? Man kann sagen, hier sind es vielleicht nur Schweine, doch wehret den Anfängen! Ich bitte um Datenschutz!"

B verweigerte die Aussage und schickte eine Kopie seines Rechtfertigungsschreibens gegenüber der (auch eingeschalteten) Verbandsgemeindeverwaltung der Staatsanwaltschaft zu.

Die Staatsanwaltschaft stellte daraufhin das Verfahren wegen Verstoßes gegen "das Datenschutzgesetz" ein, da der Vorwurf nicht nachzuweisen wäre und zitierte zur Begründung aus dem Brief des B, in dem dieser behauptete: "Im Ort ist unter Landwirten allgemein bekannt, wieviele Schweine in den einzelnen Betrieben gehalten werden." (Dieses Argument des B wurde L auch vom Landesdatenschutzbeauftragten entgegengehalten). Im übrigen könne aus der Bemerkung "ca. 40 Schweine" keineswegs zwingend geschlossen werden, daß dieser Angabe die tatsächliche Zahl 43 zugrundeliege.

Die L legte daraufhin Beschwerde ein und führte aus, daß sie erstens nicht im, sondern vor dem Ort wohne, zweitens ihr Mann keinerlei Kontakt zu den übrigen Dorfbewohnern habe und drittens ihr gegenüber B selbst zugegeben habe, daß er die Zahl aus der Viehzählung habe. Sie habe das bisher verschwiegen, da sie ihm das bei einer eventuellen Verhandlung "ins Gesicht" habe sagen sollen.

Der Generalstaatsanwalt antwortete darauf: "Es ist fraglich, ob die Zahl der im Betrieb gehaltenen Schweine als "Geheimnis" im Sinne von § 203 StGB aufzufassen ist, da ein schutzwürdiges Interesse an der Geheimhaltung nicht zu erkennen ist." Auch liege deshalb kein strafbares Verhalten vor, da B die Zahl nicht "unbefugt", sondern in einem Verwaltungsstreit zur Wahrung berechtigter Interessen der Gemeinde bekanntgegeben habe. Dies wurde ebenso für die Strafvorschrift des Landesdatenschutzgesetzes gelten. Die Beschwerde werde deshalb als unbegründet zurückgewiesen.

Fall 36 ("informatorische Anfrage"):

Nachdem der Betroffene B eine Kurzmitteilung nach § 34 I BDSG erhalten hatte, wandte er sich an die Auskunftei, die ihm über den Anfragenden keine Auskunft gab, sondern sagte, sie werde veranlassen, daß dieser ihn um 18.00 Uhr anrufen werde. Als er um 18.00 Uhr den Anruf erhielt, stellte sich heraus, daß es sein Schwager S war, der nicht verstand, warum B sich aufregte. Er habe nur wissen wollen, ob B Schulden habe, da er ja das Haus der Schwiegereltern übernehmen wollte. Da B der Meinung war, daß S zum Zeitpunkt der Abfrage wußte, daß er das Haus nicht übernehmen wollte, stellte er (10 Monate später) Strafantrag und beschuldigte S, er habe über seinen Arbeitgeber (Firma A) die Auskunft erhalten. Aufgrund der Ermittlungen der Staatsanwaltschaft stellte sich heraus, daß nicht von Firma A, sondern von Firma F die "informatorische Anfrage" erfolgte. In einem Vermerk der Staatsanwaltschaft finden sich nun folgende Aussagen:

"Sollte der Beschuldigte vom Inhalt der Auskunft Kenntnis gehabt haben, so hat er sich diese Kenntnis unter Umständen über Dritte beschafft, nicht jedoch unmittelbar "aus in Behältnissen verschlossenen Dateien" oder mittels "Abrufs" verschafft, worunter nur das technische Abrufen mittels Computers oder Terminals zu verstehen ist." Zudem fehle es an der Rechtzeitigkeit des Strafantrages. Das Verfahren sei daher nach § 170 II StPO einzustellen.

Dem Anzeigenersteller schrieb er: "Die Ermittlungen haben ergeben, daß der Beschuldigte weder sich Daten aus in Behältnissen verschlossenen Dateien verschafft noch diese Daten mittels Computers oder Terminals abgerufen hat. Bereits aus diesem Grunde scheidet eine Strafbarkeit des Beschuldigten nach § 41 Bundesdatenschutzgesetz aus. Zudem haben Sie Ihren Strafantrag nach Ablauf der ... Frist gestellt. Die Ermittlungen haben ergeben, daß einer Firma F Auskunft erteilt worden ist. Aber auch insoweit scheidet eine Strafverfolgung eines Verantwortlichen dieser Firma aus, da die Auskunft auf Grund einer schriftlichen Anfrage erfolgte und die Daten nicht in technischem Sinne abgerufen worden sind."

Fall 37 ("Bankauskunft"):

Der Betroffene B erhielt von einer Handelsauskunftei H eine Benachrichtigung nach § 34 I BDSG. Da er der Meinung war, daß zur Zeit niemand ein berechtigtes Interesse an der Auskunft haben könne, wandte er sich an den Landesbeauftragten für den Datenschutz, der das Schreiben an die Aufsichtsbehörde weiterleitete. Als diese ihm mitteilte, daß sich ergeben hatte, daß die Übermittlung unzulässig sei, sie aber aus rechtlichen Gründen den Datenempfänger nicht nennen könne, stellte B Strafantrag. Bei den Ermittlungen stellte sich heraus, daß der Inhaber I eines Bankhauses die H beauftragt hatte, wobei er als berechtigtes Interesse "Bonitätsprüfung" angegeben hatte. I war aber nicht für sich, sondern für den Kunden K, der angeblich mit B eine Geschäftsbeziehung eingehen wollte, tätig geworden. Da die geplante Geschäftsverbindung entfallen war, wurde der inzwischen von H an I gesandte Bericht nicht mehr an K weitergeleitet. Der Rechtsanwalt des I machte u. a. geltend:

"Eine mittelbare Täterschaft ist bei den sog. eigenhändigen Delikten nicht möglich. Der Tatbestand des Übermittelns im Sinne des § 41 I, 1 BDSG ist ein eigenhändiges Delikt, und zwar für die sog. speichernde Stelle. D. h. nur derjenige, der Daten speichert, kann im Sinne der vorgenannten Vorschrift auch übermitteln." Sein Mandant sei aber nicht speichernde Stelle.

Der Staatsanwalt legte in einem Vermerk seine Überlegungen dar:

Erstens sei auf H der vierte Abschnitt des BDSG anwendbar. Ein berechtigtes Interesse gem. § 32 Abs. 2 habe nicht vorgelegen, da nicht für I selbst eine Bonitätsprüfung vorgenommen werden sollte.

Zweitens sei § 41 I Nr. 1 kein eigenhändiges Delikt, weil kein unmittelbar körperlich zu vollziehender Akt notwendig sei. Es sei auf die ähnlich gelagerte Vorschrift des § 203 I StGB zu verweisen, die auch kein eigenhändiges Delikt sei.

Und drittens: "Der Umstand, daß im vorliegenden Fall der (in mittelbarer Täterschaft handelnde) Übermittler der Daten und der Dritte, an den die Daten weitergegeben werden, identisch ist, läßt den Tatbestand des § 41 Abs. I Nr. 1 BDSG nicht entfallen. Nach dem Wortlaut des § 2 Abs. II Nr. 2 BDSG ist das Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an Dritte in der Weise, daß die Daten durch die speichernde Stelle weitergegeben oder zur Einsichtnahme, namentlich zum Abruf bereitgehalten werden. Somit stellt diese Vorschrift darauf ab, daß die Daten von den Personen, die mit der Speicherung befaßt sind, an Dritte weitergegeben oder zur Einsichtnahme bereitgehalten werden. Diese Voraussetzung liegt hier vor."

Zusammenfassend lasse sich feststellen: "Der Tatbestand war zu dem Zeitpunkt erfüllt, zu dem H die Auskunft an das Bankhaus abschickte. Der Umstand, daß die zuständigen Personen der speichernden Stelle zulässigerweise Kenntnis von den Daten haben durften, ändert nichts an der Strafbarkeit des mittelbaren Täters, da sich der Täter zwar eines Werkezuges bedient, mit diesem aber nicht gleichgesetzt wird (so z. B. für den Fall der Anstiftung eines Schuldunfähigen zum Selbstmord bei Dreher RN 5 vor 211)."

Der Staatsanwalt ließ danach den I wissen, ihm werde ein Vergehen der in mittelbarer Täterschaft begangenen unbefugten Übermittlung von dem nach dem BDSG geschützten personenbezogenen Daten nach den §§ 41 I Nr. 1, 32 II BDSG vorgeworfen, er aber beabsichtige, das Verfahren nach § 153a I StPO einzustellen, falls er den Betrag von 3 000,-- DM (das entspricht etwa 20 Tagessätzen) zahlen werde. I bezahlte.

Fall 38 ("Karteikastenraub"):

Frau F betrieb in ihrem Haus einen kleinen Gewerbebetrieb dergestalt, daß sie Rohmaterialien vom Gewerbetreibenden G bezog, verarbeitete und ihm die Fertigprodukte wieder zurückgab und er sie vertrieb. Nach einiger Zeit faßten sie und ihr Mann den Entschluß, Artikel selbst zu vertreiben und liessen daraufhin eine Bekannte einen V-Versand gründen und in Illustrierten inserieren.

Etwa ein halbes Jahr später besuchte G überraschend mit drei seiner Mitarbeiter die allein anwesende F, stieß sie, nachdem sie die Türe geöffnet hatte, beiseite, ging in die Fabrikationsräume, durchwühlte Regale und nahm angeblich ihm gehörende Rohmaterialien sowie einen Karteikasten des V-Versandes mit ca. 150 Kundenadressen auf Karteikarten an sich und verschwand.

Die Eheleute stellten daraufhin Strafantrag "wegen Verstoßes nach dem Datenschutzgesetz", Diebstahl, Hausfriedensbruch und Sachbeschädigung.

Später ließ der beschuldigte G der Staatsanwaltschaft über seinen Rechtsanwalt erklären, das Konkurrenzunternehmen V-Versand werde vom Ehemann der F betrieben und die Adressen seien die seiner Kunden, weshalb er auch die Eheleute vor dem Landgericht gemäß II 1, 13 I UWG auf Unterlassung der Nutzung der Adressen verklagt habe.

Als schließlich vor dem Landgericht ein Vergleich zwischen den Parteien zustandekam, stellte die Staatsanwaltschaft das "Verfahren gegen G wegen Verstoßes gegen das UWG" gemäß § 153 I StPO mit Zustimmung des Gerichts wegen geringer Schuld ein, "weil nach dem zivilrechtlichen Vergleich nunmehr auch kein öffentliches Interesse an der weiteren Verfolgung besteht."

Fall 39 ("Telefondatenerfassung"):

In einer Zeitung erschien ein Artikel, in dem behauptet wurde, Stadtbediensteter S habe von seinem Dienstapparat aus laufend eine bestimmte Partei angerufen. Dies ergebe sich aus Computerausdrucken über die aufgezeichneten Telefongespräche. S stellte daraufhin Strafantrag gegen Unbekannt, wobei er sich nicht gegen die Praxis der computermäßigen Aufzeichnung von Telefongesprächen, sondern gegen die Übermittlung derartiger Informationen an die Presse wandte.

Nach mehreren Zeugenvernehmungen stellte die Staatsanwaltschaft das Verfahren ein: Die elektronische Speicherung der Telefongespräche stelle weder eine Verletzung des Fernmeldegeheimnisses (§ 354 I, III StGB), noch des Landesdatenschutzgesetzes dar. Soweit der Ausdruck der Presse zugespielt worden sei, hätte der Täter nicht festgestellt werden können, da der betreffende Journalist von seinem Aussageverweigerungsrecht nach § 53 I Nr. 5 StPO Gebrauch gemacht habe.

Fall 40 ("Zentralnamenskartei"):

Rechtsanwalt R vertrat den Mandanten M in einem Strafverfahren. In einem Schriftsatz an das Gericht führte er aus, daß gegen den, seinen Mandanten M belastenden, Zeugen Z bereits dreizehn Ermittlungsverfahren (u. a. wegen Falschaussage) anhängig gewesen seien und führte als Beweis die Aktenzeichen auf. Daraufhin wurde von Amts wegen ein Ermittlungsverfahren gegen Unbekannt wegen Verstoßes gegen die Strafbestimmungen des Landesdatenschutzgesetzes und § 353 b I StGB eingeleitet, da R die Aktenzeichen in dieser Form und Reihenfolge, die der auf Karteikarte in der Zentralnamensdatei entspräche, nur durch eine Person erhalten haben könnte, die Zugang zur Kartei der Staatsanwaltschaft habe. Der telefonisch unterrichtete Z stellte daraufhin schriftlich Strafantrag. Ein als Zeuge vernommener Justiz-

bediensteter J sagte aus, R, den er vom Sehen als Rechtsanwalt kenne, habe ihm gegenüber gesagt, er benötige die Karteikarte eines Mandanten, da er nicht genau wisse, um welches Verfahren es sich handele und er nur so Kontakt mit dem zuständigen Staatsanwalt aufnehmen könne. Dieser Mandant sei Z. Darauf habe er, J, dem R von der Karteikarte des Z eine Kopie angefertigt. Die Karteikarte enthielt (wie bei fast allen Staatsanwaltschaften) folgende Daten:

Name, Vorname,
Geburtsdatum, Geburtsort,
Beruf, Wohnort,
Aktenzeichen und Art des Vorwurfs bzw. Tatbezeichnung.

Nach weiteren Ermittlungen beantragte die Staatsanwaltschaft im Juli 1982 gegen R einen Strafbefehl wegen Verstoßes gegen das Landesdatenschutzgesetz, weil er sich unbefugt nicht offenkundige personenbezogene Daten verschafft habe, in Höhe von 20 Tagessätzen. Der zuständige Richter hatte aber "Bedenken gegen den Erlaß des Strafbefehls". "Das Strafrecht gehört gemäß Art. 74 GG zur konkurrierenden Gesetzgebung. Gemäß Art. 72 GG haben die Länder die Befugnis zur Gesetzgebung nur,soweit der Bund von seiner Gesetzgebung keinen Gebrauch gemacht hat. Im vorliegenden Fall gibt es ein Bundesdatenschutzgesetz mit einer Strafvorschrift in § 41. Insoweit wird das Landesrecht verdrängt."

Nachdem die Staatsanwaltschaft in einer Stellungnahme der Auffassung war, "es ist nicht anzunehmen, daß der Landesgesetzgeber das Landesdatenschutzgesetz nicht schon längst entsprechend geändert hätte, wenn die dortige Auffassung" (des Richters) "zutreffend wäre", wurde vom Richter gemäß § 408 StPO Termin zur Hauptverhandlung anberaumt, die schließlich mit einem Freispruch für R "aus tatsächlichen Gründen" endete. Es habe R kein strafbares Verhalten nachgewiesen werden können, da keine vollständige Übereinstimmung der Reihenfolge der im Schriftsatz und der auf der Karteikarte gegeben sei, so daß er nach dem Grundsatz "in dubio pro reo" habe freigesprochen werden müssen. Die von der Staatsanwaltschaft zunächst eingelegte Berufung wurde von ihr wieder zurückgenommen.

Fall 45 ("Löschungsbegehren"):

Bei einer Dienststelle der Kriminalpolizei in Niedersachsen ging Anfang Januar 1980 folgendes Schreiben des A ein, das nach Absenderangabe und Adresse lautete:

"Betr.: Antrag auf Löschung meiner personenbezogenen Daten
Bezug: 1. Aktenzeichen xy ...
2. EDV-Nr.: 007 ...

Sehr geehrte Herren!
Hiermit beantrage ich die Löschung der personenbezogenen Daten, die bezüglich meiner Person in ihrem EDV-System geführt werden.
Hochachtungsvoll"

Die Überprüfung durch die Kripo ergab, daß nur eine Kriminalakte über Trunkenheit im Straßenverkehr vorlag, und daß die Kriminalakten und EDV-Nr. einem Außenstehenden nicht bekannt sein könne, weswegen "ein Verstoß gegen den Datenschutz" anzunehmen sei. Weiter stellte sich heraus, daß der Sohn S des Antragstellers A bei der Polizei beschäftigt war und von

dem in dessen Dienststelle stehenden Terminal zwei Abfragen zur Person des A erfolgt waren. Die Kripo leitete daraufhin die Unterlagen an das Landeskriminalamt (LKA) weiter und schrieb:

"Für die Stellung des Strafantrages gemäß § 21 NDSG ist als "Herr der Daten" der Direktor des Landeskriminalpolizeiamtes Niedersachsen zuständig." Dieser stellte Anfang März Strafantrag wegen Verstoßes gegen das NDSG. Es fand sich vom LKA ein Vermerk, wonach Verstöße gegen § 21 NDSG nur auf Antrag verfolgt würden, sofern nicht ein besonderes öffentliches Interesse an der Strafverfolgung bestehe und daß als Strafantragsberechtigte sowohl der Betroffene als auch der "Herr der Daten" zu verstehen sei, welcher hier das LKA sei, da es die DV-Anlage betreibe. Bei der Vernehmung des S gab dieser unumwunden zu, daß er die Abfrage auf Drängen seines Vaters (A) getätigt hatte. Der Grund liege darin, daß nach Rückgabe des wegen eines Trunkenheitsdeliktes zeitweise entzogenen Führerscheins sein Vater wiederholt an seinem Wohnort im Straßenverkehr wegen Alkohol kontrolliert worden sei. Weiter führte er aus: "Ich wollte mit dieser Handlung auch kein Datengeheimnis brechen, sondern nur als Sohn meinem Vater helfen. Insbesondere war es mir darum gelegen, daß mein Vater als rechtschaffender Bürger nicht wegen eines einmaligen Verkehrsdelikts in dem Informationssystem von polizeilich interessanten Personen gespeichert ist."

Als daraufhin der Strafantrag vom LKA zurückgezogen wurde, stellte die Staatsanwaltschaft das Verfahren mangels Strafantrages ein. Der Verletzte, nämlich der Vater, habe keinen Strafantrag gestellt und ein öffentliches Interesse bestehe nicht. Für § 203 StGB fehle ebenfalls ein Strafantrag und für eine Verfolgung nach § 353 b StGB die Ermächtigung der obersten Landesbehörde (aus der Akte ging allerdings nicht hervor, ob sie informiert war).

Fall 46 ("Meisteranerkennung"):

Der Betroffene B beantragte im August 1978 die Meisteranerkennung gemäß § 8 II HandwO (Ausnahmebewilligung ohne Prüfung) und reichte dazu Unterlagen ein, u. a. ein staatliches Zeugnis über seine Tätigkeit bei der öffentlichen Hand. In seiner Stellungnahme Anfang Februar 1979 gegenüber der Kreishandwerkerschaft legte Obermeister O der Handwerkerinnung dar, warum sich der Innungsvorstand gegen eine Erteilung der Ausnahmebewilligung aussprach. Ende Dezember stellte B Strafantrag: "O hat persönliche Daten, die sich zweifelsfrei aus dem staatlichen Zeugnis ... ergeben, an besagte Handwerkskammer in dem oben genannten Verfahren weitergereicht. Hierin erkenne ich die Verletzung meiner persönlichen Daten."

Die Staatsanwaltschaft stellte Ende Januar 1982 das Verfahren ein: "Der Beschuldigte hat als Innungsobermeister im Rahmen der ihm in dieser Funktion zustehenden Befugnisse gehandelt. Ein unbefugtes Handeln wie es § 21 des niedersächsischen Landesdatenschutzgesetzes erfordert kann in dem Verhalten nicht erkannt werden."

Nach Beschwerde des B nahm der einstellende Staatsanwalt die Ermittlung wieder auf, kam aber wieder zum gleichen Ergebnis. Nach nochmaliger Beschwerde antwortete Ende Juli 1982 der Generalstaatsanwalt, daß das Ergebnis der Sach- und Rechtslage entspräche. Ergänzend sei darauf hinzuweisen, daß die dreimonatige Strafantragsfrist verstrichen gewesen sei.

Fall 47 ("Buchclub"):

M war Mitglied in einem englischen Buchclub B, der unter einer Adresse in Deutschland erreichbar war. Als er einige Zeit später von einem Verlag mit Sitz in Amsterdam Werbematerial erhielt und die Adresse die gleichen Charakteristika enthielt, welche er bei der Adresse für den Buchclub "eingebaut" hatte, beschwerte er sich beim Bundesbeauftragten für den Datenschutz (BfD) und stellte Strafantrag. Über die vom BfD eingeschaltete Aufsichtsbehörde wurde die Staatsanwaltschaft unterrichtet. Es stellte sich heraus, daß die Buchclubadresse in Deutschland nur die deutsche Postfachadresse des in Großbritannien ansässigen Buchclubs war. Das unter der deutschen Anschrift erreichbare Unternehmen (Einzelfirma E) leitete die Schreiben etc. nur nach Großbritannien weiter. Dort wurden sie dann in einer EDV-Anlage gespeichert. Bei der Besichtigung der Örtlichkeiten des E durch die Polizei wurde festgestellt, daß es nur sehr wenige Geschäftsräume gibt, daß keine internen Dateien oder Karteien vorhanden seien und daß die Tätigkeit für B nur einen kleinen Teil der Geschäftstätigkeit ausmacht. Die Rückfrage der Aufsichtsbehörde in Großbritannien hatte ergeben, daß B die Adressen tatsächlich weitergegeben hatte.

Die Staatsanwaltschaft stellte daraufhin das Verfahren wegen Verdachts des Verstoßes gegen das BDSG nach § 170 II StPO ein:

"Das Bundesdatenschutzgesetz umfaßt mit seinem Schutz vor Datenmißbrauch nur die Verarbeitung von Daten innerhalb der Bundesrepublik Deutschland." Dies liege nicht vor, da E, der keine Zweigniederlassung sei, keine Datei unterhalte und die Datenverarbeitung außerhalb der Bundesrepublik durch den Buchclub B nicht dem BDSG unterfalle.

Fall 48 ("Jungwählerin"):

Die kanpp 70jährige Betroffene B erhielt vor einer Wahl an ihren in Rheinland-Pfalz liegenden Zweitwohnsitz in Z von einer politischen Partei P Werbematerial für Jungwähler. Da sie der Meinung war, die Adressenübermittlung verstoße gegen "das Datenschutzgesetz", stellte sie - nach Schriftwechsel mit der Meldebehörde - Strafantrag gegen Unbekannt.

Die Staatsanwaltschaft stellte das Verfahren gemäß § 170 II StPO ein, da kein Verstoß gegen § 27 I Nr. 1 LDatG RhPf vorliege. Die Übermittlung der personenbezogenen Daten an die Partei sei nicht unbefugt erfolgt, wie sich aus der zu § 29 III LDatG RhPf erlassenen Verwaltungsvorschrift (Ministerialblatt RP 1980, 270) für die Übermittlung von Daten aus dem Melderegister an politische Parteien ergebe. Diese lautet: "Nach § 29 Abs. 3 des Landesdatenschutzgesetzes vom 21.12.1978 (GVBl. S. 749) ist es zulässig, den zu ener Bundestag-, Landtags- oder Kommunalwahl oder zu den Europawahlen in Deutschland zugelassenen Parteien und Wählergruppen auch außerhalb der Vorbereitung von Wahlen personenbezogene Daten im gesetzlich zugelassenen Rahmen zur Verfügung zu stellen."

Die Beschwerde der B wurde vom Generalstaatsanwalt zurückgewiesen. Sie sei zwar nicht Jungwähler, die versehentliche Übermittlung auch ihrer Daten sei jedoch unerheblich, da die Meldebehörde zur Übermittlung der Daten aller Wähler befugt gewesen sei.

Der Rechtsanwalt der B stellte daraufhin den Antrag auf gerichtliche Entscheidung gemäß § 172 II 1 StPO. Er führte aus, daß zum einen die Übermittlung unzulässig sei, da B in Z keinen Wohnsitz im Sinne von § 12 BWG habe, zum anderen erweitere die genannte Verwaltungsvorschrift zur sog. "Gruppenauskunft" nach § 29 III LDatG RhPf unzulässigerweise den zwingenden Rahmen des Gesetzes und stelle "eine Verwässerung des Datenschutzes" dar. Das OLG verwarf durch Beschluß den Antrag als unbegründet. Bei der Weitergabe der Jungwähleradressen sei "offenbar infolge eines Versehens, d. h. ohne Willen und Wollen", ihre Adresse übermittelt worden. Somit liege kein vorsätzliches Handeln in Bezug auf die Weitergabe der Daten der Antragstellerin (B) vor.

Fall 49 ("Flurbereinigung"):

Landwirt L erhielt die beim Katasteramt beantragten Auszüge aus dem Liegenschaftsbuch. In einer wegen eines Flurbereinigungsverfahrens angesetzten öffentlichen Versammlung unterstellte er dem Landwirt A, dieser könne deshalb gut für die Flurbereinigung eintreten, weil "nur 13 - 14 Hektar seines insgesamt 100 Hektar großen Grundbesitzes" vom Verfahren betroffen würden. A stellte daraufhin Strafantrag wegen Verstoßes gegen das Landesdatenschutzgesetz.

Das von der Staatsanwaltschaft um Stellungnahme gebetene Katasteramt gab die Rechtsgrundlagen für die Erteilung von Auskünften aus dem Liegenschaftskataster an und führte aus: "Da bei Herrn L ein berechtigtes Interesse (u. a. Verschaffung eines eigenen Überblicks über die vorhandene Besitzzersplitterung) zu unterstellen war und das Interesse der Allgemeinheit nicht entgegenstand, wurden ihm für den Bereich der Fluren 1 - 24 Eigentümerlisten, die entsprechenden Flurkarten sowie als Übersicht die Deutsche Grundkarte 1 : 5 000 ausgehändigt. Die hierfür entstandenen Kosten hat er bezahlt."

Die Staatsanwaltschaft teilte diese Stellungnahme dem A auszugsweise mit und schloß: "Bei dieser Sachlage kann ein Vergehen nach dem Datenschutzgesetz oder ein sonstiger Straftatbestand nicht festgestellt werden."

Fall 50 ("Nötigungsversuch"):

Staatsanwalt S bearbeitete das Ermittlungsverfahren gegen Kaufmann K wegen Steuerhinterziehung etc. Bei einem Gespräch erklärte K, er habe über ihn private Ermittlungen angestellt: So habe er bei der Meldebehörde über den dortigen Beamten B Auskünfte (u. a. Geburtsdatum) eingeholt, auch habe er Lichtbilder gemacht und bei Nachbarn nachgeforscht, wobei er erfahren habe, daß S beim Hausbau immer die Mehrwertsteuer bezahlt und keine Schwarzarbeiter beschäftigt habe. K bedauerte dann, nichts nachteiliges habe feststellen zu können, mit dem er S hätte unter Druck setzen können. Nachdem bei einer Hausdurchsuchung ein Notizzettel des K mit Angaben aus einem Gespräch mit B gefunden worden war, stellte S Strafantrag gegen K wegen Straftaten nach §§ 41 BDSG, 203 StGB und 353 StGB. Der als Beschuldigte vernommene B gab an, nur die alte Adresse des S, Auszugsdatum und neue Adresse, nicht aber das Geburtsdatum mitgeteilt zu haben, wie er es seit 16 Jahren beim Einwohnermeldeamt praktiziere; er war der Auffassung, daß dies nach dem Landesmeldegesetz zulässig sei. Der als Zeuge vernommene K gab an, das Geburtsdatum über eine Han-

delsauskunftei H erfahren zu haben. Die Staatsanwaltschaft stellte daraufhin das Verfahren ein: Die telefonische Bekanntgabe der Anschrift sowie das Abmeldedatum durch B sei nicht unbefugt im Sinne des Landesdatenschutzgesetzes oder § 203 StGB und § 353 b StGB erfolgt, da das Landesmeldegesetz dies erlaube. Eine Nennung des Geburtsdatums wäre unzulässig gewesen, dies sei B jedoch nicht nachzuweisen.

S legte Beschwerde ein, da auch Auskünfte über das Auszugsdatum nicht zulässig seien. Außerdem bestehe ein Schreiben der H, nach dem diese keinerlei Informationen über ihn besitze. Desweiteren gehe aus der handschriftlichen Gesprächsnotiz das Geburtsdatum hervor. Der aufgrund der wiederaufgenommenen Ermittlungen als Zeuge vernommene Geschäftsführer der Auskunftei gab an, daß K seit Jahren Kunde sei und eines Tages Auskunft über "einen S" wollte, was jedoch nicht möglich gewesen sei, da der Vorname gefehlt habe. Tage später habe dann K wieder angerufen und nun Vornamen, Geburtsdatum sowie alte und neue Anschrift mitgeteilt habe, allerdings ohne zu sagen, woher er die Informationen habe. Aus einem Vermerk der Staatsanwaltschaft geht hervor, daß nun ein hinreichender Tatverdacht angenommen wurde. Der Dienstvorgesetzte des B habe jedoch mitgeteilt, daß es bei B nach einer schweren Krebsoperation zu Funktionsstörungen von Organen gekommen sei und er sich zudem eine Infektion zugezogen habe. B liege deshalb auf der Isolierstation und eine Verhandlungsfähigkeit sei in nächster Zeit kaum zu erwarten. Die Staatsanwaltschaft stellte daraufhin das Verfahren wegen geringer Schuld nach § 152 I StPO mit Zustimmung des Gerichts ein: Möglicherweise sei B "durch Fangfragen des B überrumpelt" worden.

Fall 51 ("Nebenberuf"):

Der Angestellte A nahm bei der Firma F die Arbeit auf, kündigte aber nach einem Tag. Nach vier Monaten erhielt er von der Bausparkasse B einen zur Unterzeichnung vorbereiteten Bausparvertrag. In dem Schreiben behauptete B, daß F zum Abschluß des Vertrages und Überweisung der monatlichen Prämie (vermögenswirksame Leistungen) bereit sei. Da B dem A die Auskunft, woher sie die Adresse habe, verweigerte, stellte A Anfang Dezember 1980 bei der Polizei Strafantrag wegen "Verstoßes gegen das Datenschutzgesetz". Als die Kripo Anfang März 1981 die Firma F aufsuchte, wurde ihr mitgeteilt, daß man dem Programmierer P schon im Dezember fristlos entlassen habe, da er eine Änderung am Programm dergestalt vorgenommen habe, daß er das Suchkriterium "welche Personen beziehen keine vermögenswirksame Leistungen" einfügte und sich eine Liste dieser Personen ausdrucken ließ. Diese Personen seien daraufhin von P, der zugleich nebenberuflich Vermittler der B war, über einen Strohmann angeschrieben worden. Auf Beschwerden hin sei die Tat durch die Firma aufgedeckt worden. P war geständig. Daraufhin wurden alle 33 Personen der Liste angeschrieben. Fünf stellten Strafantrag, achtzehn verzichteten, fünf behielten ihn sich vor und fünf antworteten nicht; eine war unbekannt verzogen. Es stellte sich heraus, daß es zu drei Vertragsabschlüssen gekommen war, die jedoch nach Aufdeckung der Tat storniert worden waren. Die Staatsanwaltschaft stellte das Verfahren im Dezember 1981 wegen Verstoßes gegen das BDSG gemäß § 153 I StPO mit Zustimmung des Gerichts ein: "Angesichts dessen, daß die Tat folgenlos blieb und ohne besondere kriminelle Intensität verübt wurde, ist das Maß der Schuld als gering anzusehen. Da der Beschuldigte nach der Tat von der Firma F entlassen wurde und die Tat nunmehr auch schon 1 Jahr zurück-

liegt, besteht kein öffentliches Interesse an der Verfolgung mehr. Hinzu kommt, daß die Akten nach Abschluß der umfangreichen Ermittlungen bei der Übersendung an die Staatsanwaltschaft verlorengingen und auch bei der Polizei keine Mehrfertigung der Akten vorliegt. Unter diesem Gesichtspunkt erscheint es unverhältnismäßig, die Ermittlungen von neuem durchzuführen."

Fall 52 ("Lebenslauf")

Der in der Justizvollzugsanstalt (JVA) einsitzende Häftling H bekam eines Tages von seinem Zellengenossen Z bestimmte Gegebenheiten aus seinem Leben vorgehalten. Ferner machte Z gegenüber anderen Gefangenen Andeutungen über Privatleben, Schulden und Vorstrafen des H und las dabei teilweise aus Blättern vor. H berichtete später, daß ihm gegenüber einer der "Zuhörer" behauptet habe, er hatte erkannt, daß es sich teilweise um Unterlagen einer bestimmten Auskunftei gehandelt habe. Schließlich gelangten zwei eng mit Schreibmaschine beschriebene Blätter, gespickt mit persönlichen, beruflichen und finanziellen Daten, vom Tag der Geburt bis zur Inhaftierung, in die Hände der Anstaltsleitung. Sie erstattete daraufhin Strafanzeige und stellte Strafantrag gegen Unbekannt.

Da die Vernehmungen des Beschuldigten Z und zweier außerhalb der JVA sich befindlichen Zeugen keine Klärung brachte, stellte - nachdem nun der fehlende Strafantrag des H vorlag - der Staatsanwalt, knapp 2 Monate nach Anzeigeneingang, das Verfahren ein: Es hätte nicht geklärt werden können, woher Z die Unterlagen habe und es hätten keine weiteren Ermittlungen mehr getätigt werden können. Möglicherweise habe sich Z der Teilnahme an einer Straftat schuldig gemacht, da die Haupttat jedoch nicht bewiesen sei, könne Z auch insoweit nicht verfolgt werden.

Deroben erwähnte "Zuhörer" wurde nicht vernommen und auch bei der benannten Auskunftei waren keine Ermittlungen angestellt worden, womit die Frage, ob es sich wirklich um Unterlagen einer Auskunftei gehandelt hat, offenblieb.

Fall 53 ("Polizeiausdrucke"):

In der Zeitung Z war über ein bestimmtes polizeiliches Computer-Programm ein kritischer Bericht mit Bildern von geheimzuhaltenden Unterlagen erschienen. Am selben Abend besuchten zwei Redakteure der Z einen gewissen A in dessen Wohnung, da dieser dort angeblich weitere gestohlene Computer-Ausdrucke (die er von einem Polizeibeamten habe) zum Kauf anbot. Nachdem die Verhandlungen anscheinend für beide Seiten nicht den gewünschten Verlauf genommen hatten, verließen die Redakteure die Wohnung. Später riefen sie die Polizei an und behaupteten, A habe sie bezüglich der Ausdrucke zu erpressen versucht, worauf noch am selben Abend bei A eine Hausdurchsuchung vorgenommen wurde. Als dort die Adresse des Polizeibeamten P gefunden wurde, wurde A vorläufig festgenommen, nach seiner Vernehmung am nächsten Tag aber wieder freigelassen. Eine Durchsuchung der Wohnung des P blieb erfolglos. Nach umfangreichen Ermittlungen und Zeugenvernehmungen in dem sich A und die Redakteure (die sich teilweise auf ihr Zeugnisverweigerungsrecht beriefen) wechselseitig beschuldigten, wurde das Verfahren gemäß § 170 II StPO eingestellt. Sowohl A als auch P seien keine Straftaten nachzuweisen, zumal die jeweiligen Angaben der beiden Redakteure nur in bezug auf die Teile zu den Aussagen des A zusammenpaßten, ansonsten aber in vielen Dingen erhebliche Widersprüche aufwiesen.

Fall 54 ("Schuldnerkartei"):

Der Anzeigenerstatter beklagte die nachlässige Löschung der Eintragungen in das Schuldnerverzeichnis (§ 915 ZPO), die dazu führe, daß man auch noch die eigentlich gelöschten Daten lesen könne. Nach schriftlicher Stellungnahmen der betroffenen Bediensteten und ihres Vorgesetzen wurde das Verfahren nach § 170 II StPO mangels Tatverdacht eingestellt, da die ungenügende Schwärzung nicht vorsätzlich erfolgt sei, der fahrlässige Verstoß gegen das Landesdatenschutzgesetz jedoch nicht stafbar sei. Im übrigen sei das Problem gelöst, da "jetzt ein starker schwarzer Filzstift gebraucht wird, der alles Gelöschte unlesbar schwärzt".

Fall 55 ("Krankheitsdaten"):

Die Betroffene B erhielt im Mai eine Verfügung des Landkreises als Strassenverkehrsbehörde, in der ihr die Fahrerlaubnis gem. § 4 StVG i. V. mit § 15 b StVZO entzogen wurde, da sie "nach den hier vorliegenden Unterlagen" stationär in einer Krankenanstalt zur Vorbereitung einer Behandlung nach dem Psychatriekrankengesetz, deren Einweisung laut ärztlichem Gutachten wegen ihrer Alkoholerkrankung dringend erforderlich gewesen sei, eingeliefert worden war. "Aufgrund der aus dem Gutachten gewonnenen Erkenntnisse" sei ihre Kraftfahreignung nicht mehr gegeben und ihrer Fahrerlaubnis zu entziehen. Der Anwalt der B schickte Kopien der Verfügung und seines Widerspruches an die Staatsanwaltschaft und bat um Überprüfung nach § 21 NDSG, ob ärztliche Unterlagen unter Mißachtung des § 10 I 2 NDSG weitergeleitet worden seien und ob ein Einschreiten von Amts wegen geboten sei, da er sonst Strafantrag stellen würde. Gleichzeitig informierte er den niedersächsischen Datenschutzbeauftragten.

Die Staatsanwaltschaft stellte das Verfahren mangels Tatverdacht ein und schrieb dem Anwalt der B: "Ich habe nicht im einzelnen ermittelt, auf welche Weise das Straßenverkehrsamt des Landkreises ... in den Besitz der Unterlagen gekommen ist, weil es meines Erachtens nicht darauf ankommt. Denn nach § 10 NDSG dürfte die Weitergabe entgegen Ihrer Auffassung rechtmäßig gewesen sein".

Der Datenschutzbeauftragte schrieb, daß die Daten aus Akten und nicht aus einer Datei weitergegeben seien und daß das NDSG vom organisatorischen Behördenbegriff ausgehe, so daß die verschiedenen Ämter eines Landkreises nur Teile einer speichernden Stelle seien. Maßstab sei so ausschließlich § 203 I Nr. 1 StGB, jedoch sei dabei die Befugnis zur Offenbarung aus dem Gesichtspunkt des rechtfertigenden Notstandes (§ 34 StGB) gegeben (BGH NJW 1968, 2288).

Fall 56 ("Geschäftsfreundin"):

Herr A lebte getrennt von seiner Ehefrau E und war mit Frau F befreundet. Diese erhielt im Februar 1978, mit der gleichzeitigen Bitte um Selbstauskunft, eine Benachrichtigung von der Handelsauskunftei H gemäß § 34 I BDSG. Als F von ihrem Auskunftsrecht nach § 34 II BDSG Gebrauch machte, erfuhr sie, daß folgende Daten über sie gespeichert waren:

"Auskunft über Frau F, S-Straße, S-Stadt:

Allgemeines:
Wie unsere Erkundigungen ergeben haben, soll Frau F bei der Firma X in S-Stadt in einer kaufm. Position tätig sein. Ohne Verletzung der gebotenen Diskretion war es leider nicht möglich, Zahlen über die Höhe der mtl. Bruttobezüge von Frau F zu erhalten.

Persönliches:
F wurde ca. 19xx geboren. Sie ist beschäftigt wie oben angegeben. In persönlicher und fachlicher Hinsicht findet sie eine gute Beurteilung.

Vermögenslage:
Haus- und Grundeigentum, soweit bekannt, ist für F nicht eingetragen. Die Räumlichkeiten in S-Straße, S-Stadt sind gemietet. Hier ist ein mtl. Mietzins von etwa DM x aufzubringen. Die wirtschaftlichen Verhältnisse erscheinen als gut und geordnet.

Krediturteil:
Negative Krediterfahrungen sind nicht bekannt geworden. Man hat keinen Grund, von einer Geschäftsverbindung abzuraten."

Diese Daten waren jedoch zum größten Teil falsch. Zwei Wochen später besuchte A seine Ehefrau E, die ihm den Umgang mit F vorhielt und dazu die gleichen falschen Daten wie im Auskunftsbogen nannte. Als F dies erfuhr und H ihr Schreiben und schließlich auch dieses ihres Rechtsanwaltes mit der Bitte um Überprüfung, ob ein berechtigtes Interesse vorgelegen habe, unbeantwortet ließ, stellte F Strafantrag gegen E, sowie gegen Mitarbeiter der H und Unbekannt.

Da H die ihr zugegangene Anfrage (in der um Informationen über F nachgesucht wurde) nicht herausgab, wurde es bei einer Hausdurchsuchung beschlagnahmt. Es stellte sich heraus, daß Prokurist P über seine Firma die Auskünfte bei H eingeholt hatte, nachdem er vom Handelsvertreter V, den er persönlich kannte, darum gebeten worden war. V wiederum kannte Herrn A und seine Ehefrau E und bat den P auf Bitten von E um die Auskunft. Sowohl V als auch P wußten, daß E die Auskunft für ihren persönlichen Gebrauch benötigte. Als die Staatsanwaltschaft Anfang Januar 1979 der F den Sachverhalt mitteilte (P sei der unbefugten Abrufung geschützter Daten verdächtigt) zog diese ihren Strafantrag gegen P zurück, worauf das Verfahren gegen ihn eingestellt wurde. Im Juli 1979 wurde schließlich das Verfahren gegen E und V "aus subjektiven Gründen" eingestellt. Es sei nur der vorsätzliche Verstoß nach dem Datenschutzgesetz strafbar. "Ein solches vorsätzliche Verhalten ist jedoch E und V angesichts der neuen Regelung durch das Datenschutzgesetz nicht mit der für eine Anklageerhebung erforderlichen Sicherheit nachzuweisen."

Fall 57 ("Verlobtenfinanzen"):

Behördenangestellte A war mit dem Betroffenen B verlobt. Da sich dieser zwar einerseits in ständigen Geldschwierigkeiten befand und sie den Eindruck hatte, er verschweige ihr etwas, sie andererseits aber zu heiraten gedachten, wandte sie sich an ihre Feundin F. Diese meinte, es müsse doch möglich sein festzustellen, wie es um den B in finanzieller Hinsicht stünde. Kurze Zeit später warnte F die A vor B, da seine Angaben nicht zuträfen, wie sie vom Dritten D, der beim Unternehmen U beschäftigt sei, und der für sie über U eine Auskunft eingeholt habe, erfahren habe. A machte daraufhin dem B Vorhaltungen. Nach weiteren Vorkommnissen zerbrach die Beziehung und B stellte (zunächst) Strafantrag gegen das Unternehmen U (später auch gegen A). Nach umfangreichen und langwierigen Ermittlungen stellte die Staatsanwaltschaft das Verfahren gegen Mitarbeiter des Unternehmens U mangels Aufklärbarkeit ein. Das Verfahren gegen A, die bei der Vernehmung behauptete, sie habe durch Täuschung der Auskunftei die Information erlangt, wurde mit Zustimmung des Gerichts gem. § 153 a I StPO eingestellt. Aus einem Vermerk der Staatsanwaltschaft geht weiter hervor, welche Informationen über B weitergegeben wurden:

1. zwei Haftbefehle zur Erlangung der eidesstattlichen Versicherung,
2. Kredit in bestimmter Höhe bei einer Bank,
3. Kündigung eines anderen Kredits,
4. Ohnabtretungen (und Höhe).

Darunter notierte der Staatsanwalt: Das Landesdatenschutzgesetz kann nicht in Betracht kommen, da dieses "nur Daten, die von Behörden oder sonstigen öffentlichen Stellen gespeichert werden" schützt. "Bei den unter 2. bis 4. aufgeführten Daten handelt es sich um persönliche Daten, die vom Bundesdatenschutzgesetz geschützt sind". Als B gegen die oben erwähnte Einstellung Beschwerde einlegte, wurde A als Zeugin vernommen. Sie gab nun zu, von F über D die Informationen erhalten zu haben. Daraufhin wurden D und F angeklagt. D habe unbefugt vom BDSG geschütze personenbezogene Daten, die nicht offenkundig sind, abgerufen und übermittelt, F habe die Daten unbefugt übermittelt. Nachdem der Hauptverhandlungstermin anberaumt war, legte D ein schriftliches Geständnis ab, daß er auch im Termin wiederholte. Auch F war geständig. Es erfolgte eine Einstellung nach § 153 a II StPO, wobei (wie aus einem Vermerk hervorging) die Höhe des Geldbetrages bei D 20 Tagessätzen und bei F 10 Tagessätzen entsprach.

Fall 58 ("Baukasse"):

Die Angestellte A führte seit Jahren zuverlässig und beanstandungsfrei bei der Baufirma B die Kasse. Eines Tages kam sie zum Prokuristen P und erklärte, daß mit der Kasse etwas nicht stimme. Prokurist P nahm zunächst an, daß irgendwelche Belege verlegt worden seien und machte sich keine Gedanken. Als A wenige Wochen später meldete, daß Geld in der Kasse fehle und dabei nervös und zerfahren schien, riet ihr P, sofort Uralub zu machen, was sie dann tat. Als zwei Tage später der Freund F der A nach dem Grund fragte, erklärte ihm P die Angelegenheit. Bei der Überprüfung, zu der der Bankdirektor B hinzugezogen wurde, stellte sich heraus, daß A wahrscheinlich mehrere Tausend Mark entwendet haben mußte. P glaubte nun, daß bei der A seit ihrem Zusammenziehen mit F in eine gemeinsame Wohnung eine "Verhaltenswende" vorlag. Er bat deshalb B über den F nähere Informationen bei einer Auskunftei einzuholen. Dabei stellte sich heraus, daß

F Schulden hatte und eine eidesstattliche Versicherung hatte abgeben müssen. Als gegen A Strafanzeige wegen Untreue gestellt wurde, wurde ihr nebenbei mitgeteilt, daß man sich über ihren Freund F erkundigt habe. Als sie ihm dies erzählte, wandte er sich an den Landesbeauftragten für den Datenschutz, der ihn an die Aufsichtsbehörde verwies. Als diese feststellte, daß wahrscheinlich eine unbefugte Übermittlung vorlag, stellte F Strafantrag. Bei den Ermittlungen stellte sich heraus, daß B auf Veranlassung des P über die Bank bei der er angestellt war, Informationen über den F eingeholt und an P weitergegeben hatte. Die Staatsanwaltschaft stellte daraufhin mit Zustimmung des Gerichts das Verfahren gegen B und P gemäß § 153 a I StPO ein: B habe die Kreditwürdigkeit des F erfragt und die betreffenden Daten erhalten, wobei er zur Darlegung des berechtigten Interesses wahrheitswidrige Angaben gemacht habe. Er habe sich dadurch eines Vergehens der unbefugten Übermittlung nicht offenkundiger vom Bundesdatenschutzgesetz geschützten personenbezogener Daten schuldig gemacht. P wurde eine Anstiftung zur unbefugten Übermittlung vorgeworfen. Aus einem Vermerk der Staatsanwaltschaft geht hervor, daß bei der Höhe des Geldbetrages bei B von etwa 20 Tagessätzen, bei P von 15 Tagessätzen ausgegangen worden ist. B und P bezahlten.

Fall 59 ("Nachbarstreitigkeiten"):

Rentner R, der Betroffene B und seine Familie, sowie die Eheleute E wohnten in einem Haus, das den Eheleuten E gehörte. Zwischen B einerseits und E und R andererseits kam es immer wieder zu Auseinandersetzungen. Eines Tages entdeckte B, der mit R eine Doppelgarage benutzte, auf dem Beifahrersitz des Autos des R ein Schreiben der Handelsauskunftei H. Durch die geschlossenen Scheiben konnte er erkennen, daß es sich um eine ihn betreffende Kreditauskunft in Höhe von 20 000,-- DM handelte. Es hatte folgenden Inhalt:

"Auskunft über B, S-Straße, Z-Stadt:

Persönliches:	B wurde am x.x.19xx geboren. Er ist mit C, geborene D verheiratet und Vater von 3 Kindern.
Beurteilung:	In persönlicher Hinsicht ist Nachteiliges nicht bekannt. Die Eheleute kamen am x.x.19xx von S-Stadt, X-Straße zugezogen.
Tätigkeit:	B ist Industriekaufmann und als Regionalmanager für die X-Bank tätig.
Grundeigentum:	Haus- und Grundeigentum ist nicht erkennbar, die Wohnung wurde gemietet. Die Ehefrau gilt als Alleinerbin von Liegenschaften in S-Stadt und T-Stadt.
Sonstiges Vermögen:	Einige Werte wurden in die Einrichtung investiert.
Zahlungsweise:	Bisher erschienen die wirtschaftlichen Verhältnisse in Z-Stadt (= gegenwärtiger Wohnort) geordnet, Zahlungsbeanstandungen liegen hier nicht vor.
Bankverbindung:	Z-Bank in V-Stadt
	- ohne Vermögensschätzung -

Angefragter Kredit 20 000,-- DM erfordert ausreichende Sicherheiten. Es wurden noch weitere Ermittlungen eingeleitet, sollten diese für Sie wissenswertes ergeben, erhalten Sie eine Ergänzung."

B holte daraufhin die Polizei, die das Schriftstück begutachtete und den R zur Herausgabe aufforderte, was dieser zunächst ablehnte. Die wenige Tage danach bei R vorgenommene Hausdurchsuchung blieb erfolglos, jedoch konnte bei den Eheleuten E das Auskunftsschreiben sichergestellt werden. B stellte Strafantrag.

Es zeigte sich, daß R nebenbei für die Kreditbeschaffungs-GmbH K arbeitete, indem er Hypotheken vermittelte. Da dabei üblicherweise immer zuerst eine Anfrage bei H vorgenommen wurde, besorgte der Geschäftsführer G der K dem R bedenkenlos eine Auskunft über B und stellte R die Kosten von ca. 50,-- DM in Rechnung. Nach Aufdeckung dieses Sachverhaltes wurde antragsgemäß Strafbefehl gegen Herrn und Frau E sowie R in Höhe von jeweils 20 Tagessätzen erlassen:

"Sie werden beschuldigt, gemeinschaftlich handelnd, unbefugt vom Bundesdatenschutzgesetz geschützte personenbezogene Daten, die nicht offenkundig sind, abgerufen zu haben. §§ 41 I Nr. 2 BDSG, 25 II StGB."

Alle drei legten Einspruch ein, wobei u. a. geltendgemacht wurde, daß B in die Einholung der Auskunft eingewilligt habe. Dies bestritt B. In der Hauptverhandlung konnte nun den die Aussage verweigernden Eheleuten E nicht nachgewiesen werden, daß sie R beauftragt haben, zumal dieser behauptete, allein gehandelt zu haben und erst nach Erscheinen der Polizei das Auskunftsschreiben an die Eheleute E weitergegeben zu haben. Die Eheleute E wurden somit freigesprochen. R wurde wegen "unbefugten Abrufens geschützter personenbezogener Daten nach § 41 I Nr. 2 BDSG" zu der Geldstrafe von 10 Tagessätzen verurteilt. Auf die Berufung des R wurde er vom Landgericht aus Rechtsgründen freigesprochen. Das LG führte aus:

"Das Verhalten des Angeklagten wird von den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) nicht erfaßt. Danach ist Aufgabe des Datenschutzes, durch den Schutz personenbezogener Daten vor Mißbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange des Betroffenen entgegenzuwirken (§ 1 Abs. I BDSG). Das Gesetz schützt personenbezogene Daten, die in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden (§ 1 Abs. II BDSG).

Die dem Angeklagten in der eingeholten Auskunft mitgeteilten Daten sind zwar personenbezogene Daten im Sinne des BDSG, da es sich bei ihnen um Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten natürlichen Person handelt (§ 2 Abs. I BDSG). Das Gesetz erfaßt aber nicht jede Art der Verarbeitung und Benutzt von Daten, sondern nur diejenigen, die sich in der Form von Speichern, Übermitteln, Verändern und Löschen in oder aus Dateien vollzieht (vgl. Ordemann/Schomerus, BDSG 2. A. Anm. 1.2. zu § 1). Deshalb sind Straftaten im Sinne dieses Gesetzes auch nur die Übermittlung oder Veränderung oder das Abrufen oder das sich aus in Behältnissen verschlossenen Dateien verschaffen (§ 41 Abs. I BDSG). Das Verhalten des Angeklagten erfüllt die genannten Tatbestandsmerkmale nicht. Der Angeklagte hat keine Daten verändert. Nach der Sachlage hat der Angeklagte sich auch keine geschützten personenbezogenen Daten aus in Behältnissen verschlossenen Dateien verschafft.

Der Angeklagte hat auch nicht abgerufen. Das Abrufen im Sinne des Gesetzes ist nicht jeder Vorgang des Sichbeschaffens, sondern eine besondere Form, bei der personenbezogene Daten aus automatisierten Datenverarbeitungsanlagen durch technische Mittel entnommen, nämlich angerufen, werden (Ordemann/Schomerus Anm. 1.2.3. zu § 41). Auch ein Übermitteln der Daten kommt nicht in Betracht, da darunter nicht jede Form der Bekanntgabe zu verstehen ist, sondern nur die Bekanntgabe gespeicherter Daten an einen Empfänger, der die Daten wiederum in einer Datei speichert. Werden die Daten beim Empfänger nicht in einer Datei gespeichert, so ist eine Weitergabe durch diesen auch keine Übermittlung im Sinne des Gesetzes. Sie werden bei ihm frei verfügbar (Ordemann/Schomerus Anm. 2.2 zu § 2). Die Bestimmungen des Bundesdatenschutzgesetzes finden deshalb auf den vorliegenden Fall keine Anwendung. Die Voraussetzungen des § 203 StGB sind ebenfalls nicht gegeben. Da somit eine Straftat im prozessualen Sinne nicht vorliegt, kommt auch eine mittelbare Täterschaft des Angeklagten oder eine Beteiligung in Form der Anstiftung oder Beihilfe für die Person des Angeklagten nicht in Betracht."

Die Staatsanwaltschaft legte zunächst Revision ein, weil "die Feststellungen der Kammer, mit denen sie das Tatbestandsmerkmal des "Abrufens" verneint, deswegen fehlerhaft sind, weil hinreichende Ausführungen zum Problem der mittelbaren Täterschaft fehlen." ... "Es ist davon auszugehen, daß sehr wohl bei H die personenbezogenen Daten aus einer automatisierten Datenverarbeitungsanlage durch technische Mittel entnommen worden sind, daß also von dem bei dieser Firma zuständigen Sachbearbeiter die entsprechenden Daten abgerufen worden sind." ... "Die Ausführungen der Kammer lassen vermuten, daß sie § 41 Bs. 1 Nr. 1 1. Alternative des Bundesdatenschutzgesetzes für ein eigenhändiges Delikt hält. Eine erartige Auslegung geht aber am Sinn und Zweck der Strafbestimmung vorbei. Es liegt nämlich auf der Hand, daß in einem Unternehmen, das über entsprechende Datenverarbeitungsanlagen verfügt, derjenige, der den "unmittelbaren Zugriff" auf die Daten durch den technischen Vorgang des Abrufens hat, eine eher untergeordnete Rolle spielt und auf Anweisung handelt. Er wird in vielen Fällen von der Rechtmäßigkeit der Anordnung ausgehen können und deswegen beim "Abrufen" der Daten gutgläubig handeln. Derjenige im Unternehmen aber, der die Macht hat, die entsprechenden Anweisungen zu geben, könnte sich in diesem Falle nie strafbar machen, da er selbst "abruft" und Anstiftung oder Beihilfe wegen der Gutgläubigkeit des Vordermannes ausscheiden. Genauso wenig ließen sich diejenigen Fälle strafrechtlich fassen, bei denen - wie im vorliegenden Fall - sich Dritte, nicht in der Auskunftei beschäftigte, durch unrichtige, ein berechtigtes Interesse nur vorspiegelnde Anfragen, Auskünfte besorgen. Wollte man die genannte Vorschrift als eigenhändiges Delikt auslegen, so bliebe demnach eine vom Gesetzgeber ersichtlich nicht gewollte Lücke der Straflosigkeit für eine Vielzahl von Fällen."

Die StA beim OLG schloß sich diesen Ausführungen an. Später zog dann die Staatsanwaltschaft die Revision ohne Angabe von Gründen zurück.

Fall 60 ("Erbschaftsstreit"):

Mutter M hatte einen mehrfach vorbestraften Sohn V und einen Stiefsohn S. Als es wegen einer Erbschaft zu Streitigkeiten zwischen V und S sowie zwischen M und V kam, beschloß M, um dem S zu helfen, Einblick in die bei der Auskunftei A über V vorhandenen Vermögensunterlagen zu nehmen. Dazu legte sie A gefälschte Kopien vor (was A nicht bemerkte). Als V davon durch Zufall erfuhr, stellte er Strafantrag. Nach umfangreichen Ermittlungen beantragte die Staatsanwaltschaft den Erlaß eines Strafbefehls wegen Verstosses gegen § 41 I Nr. 1 in Verbindung mit § 32 II BDSG in Höhe von 40 Tagessätzen. Bevor er jedoch vom Richter unterzeichnet wurde, zog V den Strafantrag gegen seine Mutter M zurück.

Fall 61 ("Doppelhaushälfte"):

Kaufmann K erwarb eine Doppelhaushälfte und zog dort ein. Da er näheres über seinen Nachbarn N wissen wollte, bat er im Namen seiner Firma die Handelsauskunftei H um Auskunft über N, da er mit ihm in eine nähere geschäftliche Beziehung treten wolle. Als N von H die Mitteilung gemäß § 34 I BDSG erhalten hatte, schaltete er die Aufsichtsbehörde ein, die ihm mitteilte, daß eine unzulässige Datenübermittlung vorgelegen habe, sie aber den Datenempfänger nicht nennen dürfe. Darauf stellte N Strafantrag gegen Unbekannt.

Der Rechtsanwalt des K schrieb im Laufe der Ermittlungen daraufhin, daß sein Mandant ein Schwerkranker mit ausgeprägtem Ruhebedürfnis sei und er deshalb mehr über N habe erfahren wollen. Außerdem sei K bezüglich des Gemeinschaftseigentums am Haus Gesamtschuldner nach § 426 BGB, weswegen ein berechtigtes Interesse nach § 32 II BDSG gegeben sei.

In ihrer Abschlußverfügung beschudligte die StA den K, unbefugt die Handelsauskunftei durch wahrheitswidrige Angaben zur Herausgabe der personenbezogenen Daten von N veranlaßt zu haben und dadurch gegen § 41 BDSG verstoßen zu haben. Wegen geringer Schuld könne jedoch das Verfahren nach § 153 a StPO nach Zahlung eines Geldbetrages (die Höhe entsprach etwa 20 Tagessätzen) eingestellt werden. K bezahlte.

Fall 62 ("Kontaktaufnahme"):

Der mit seinem Vater V zerstrittene selbständige Verlagskaufmann K beauftragte unter dem Namen seiner Firma die Handelsauskunftei H Erkundigungen über V einzuziehen, da die Firma eine "neue Verbindung" eingehen wolle. Als V durch die Benachrichtigung (§ 34 I BDSG) von den Erkundigungen der H erfuhr, schaltete er die Aufsichtsbehörden ein und stellte schließlich, als ihm mitgeteilt wurde, es läge wahrscheinlich eine unzulässige Datenübermittlung vor, der Name des Datenempfängers dürfe aber nicht genannt werden, Strafantrag (den er auch noch aufrechterhielt, als er erfuhr, daß es sein Sohn war). Die Staatsanwaltschaft teilte dem K mit, er habe zwar unbefugt personenbezogene Daten abgerufen und damit gegen § 41 BDSG verstoßen, wegen geringer Schuld würde sie aber das Verfahren nach § 153 a StPO einstellen, wenn er einen bestimmten Geldbetrag (die Höhe entsprach etwa 20 Tagessätzen) bezahle. K überwies den Betrag.

Fall 63 ("Restrisiko"):

Oberregierungsrat O kaufte im Frühjahr 1980 bei der Bettenfirma B Bettwäsche im Werte von 530,-- DM. Dazu kamen 110,-- DM für Änderungen dazu, die, entsprechend den persönlichen Wünschen des O, von der Firma B durchgeführt werden sollten. O leistete eine Anzahlung von 250,-- DM, der Restpreis von 290,-- DM sollte bei Lieferung der geänderten Wäsche erfolgen. Wenige Tage später wurden bei den Nachbarn des O Vermögensauskünfte über ihn eingeholt und zwei Wochen nach Kauf erhielt er ein Schreiben der Handelsauskunftei H, in dem ihm mitgeteilt wurde, daß Daten über ihn gespeichert seien. Auf seine Bitte, zu überprüfen, ob beim Anfragenden, von dem O nicht wußte, wer er war, da er zwischen seinem Kauf und der Benachrichtigung der K keinen Zusammenhang sah,wirklich ein berechtigtes Interesse zugrundelag, antwortete H drei Monate später und legte die nachfolgenden Auskunftserteilung bei:

Name:	O wurde etwa 19xx geboren. Er ist verheiratet.
	Die persönliche Beurteilung lautet einwandfrei.
Beruf:	Der Beurteilte ist Oberregierungsrat beim xx. Er soll im X-Ministerium tätig sein. Eine Bestätigung hierüber konnten wir nicht erhalten.
Vermögenslage:	Die Wohnung an der obigen Anschrift gilt als Eigentum der Eheleute O. Der Verkehrswert wird auf ca. x DM geschätzt. Die Belastungen sind nicht bekannt.
	Überprüfung der Angaben zum Immobilieneigentum durch Grundbucheinsicht nicht möglich.
	Eine gut bürgerliche Wohnungseinrichtung soll vorhanden sein.
	Die finanziellen und wirtschaftlichen Verhältnisse zeigten sich bisher als geordnet.
Banken:	ohne Selbstbefragung nicht feststellbar.
Zahlungsweise:	nichts Nachteiliges bekannt.

Da die Auskunft der H zur Frage, ob ein berechtigtes Interesse vorlag, den O nicht befriedigte, wandte er sich an den Landesbeauftragten für den Datenschutz. Dieser leitete sein Schreiben an die Aufsichtsbehörde weiter, die ihm (später) mitteilte, daß ein berechtigtes Interesse im Sinne von § 32 II BDSG "nicht nur bei Kreditentscheidungen im engeren Sinne, sondern auch z. B. bei Werkverträgen mit Teilzahlung zu bejahen" sei. O durchsuchte daraufhin seine Belege und fand als Werkvertrag nur den der Firma B und sandte ihn an die Aufsichtsbehörde mit der Bemerkung, daß er sich nicht im entferntesten denken könne, daß dies Anlaß für die Auskunft gewesen sein könnte. Mit Schreiben vom 23. März 1981 an H, das O in Kopie erhielt, antwortete die Aufsichtsbehörde:

"Nach unserer Auffassung lag der Anfrage über O kein berechtigtes Interesse zugrunde. Zwar bestimmt der Gesetzgeber keine konkrete Kredithöhe, ab der ein berechtigtes Interesse bejaht werden kann, daraus kann aber keineswegs gefolgert werden, jedes noch so gerinfügige unternehmerische Rechtsrisiko könne die Übermittlung personenbezogener Daten rechtfertigen. Der allgemeine Grundsatz der Verhältnismäßigkeit ist selbstverständlich auch hier zu beachten. Er gilt vor allem dann, wenn aufgrund der Anfrage Nachbarauskünfte eingeholt werden."

O stellte daraufhin Strafantrag gegen H. Die Staatsanwaltschaft beendete das Verfahren nach § 170 II StPO mit folgender Begründung:

"Das Ermittlungsverfahren war einzustellen, daß H ein Verstoß gegen § 41 BDSG letztlich nicht nachzuweisen war, wenn auch das Vorgehen der H erheblichen Bedenken begegnet." ... "Im vorliegenden Fall fehlt es an einem berechtigten Interesse des Empfängers." ..."Ein Sicherungsinteresse im Bezug auf 390.-- DM kann die Übermittlung der in Frage stehenden personenbezogenen Daten nicht rechtfertigen. Es ist vielmehr davon auszugehen, daß nicht jedes auch noch so geringfügige unternehmerische Rechtsrisiko die Übermittlung personenbezogener Daten rechtfertigen kann, sondern daß auch insoweit der allgemeine Grundsatz der Verhältnismäßigkeit zu beachten ist" Zur glaubhaften Darlegung des berechtigten Interesses vertrat der Staatsanwalt folgende Meinung:

"Eine Anfrage ohne jeglichen Zusatz über den Umfang des Sicherungsinteresse stellt keine schlüßige Darlegung des berechtigten Interesses dar und ist somit auch keine glaubhafte Darlegung im Sinne des § 34 Abs. 2 BDSG. Aus dem Wort "Kreditanfrage" geht eben gerade nicht hervor, ob die Höhe des Sicherungsinteresses ein berechtigtes Interesse des Anfragenden an der Übermittlung von personenbezogenen Daten begründet." Einen Verstoß gegen § 41 BDSG verneinte der Staatsanwalt dann aber doch, da zwischen Firma B und H langjährige, beanstandungsfreie, geschäftliche Beziehungen bestanden und H deshalb vom Bestehen eines entsprechenden Sicherungsinteresse hätte ausgehen dürfen. Ferner sei aufgrund dieser speziellen Beziehungen den Anforderungen an die Glaubhaftmachung genüge getan.

Fall 64 (Ehevermittler):

Um Kunden für sein schlecht gehendes Ehevermittlungsinstitut zu bekommen, annocierte der Inhaber I, daß eine Filmproduktionsgesellschaft Fotomodelle suche. Die zugesandten Fotos verwandte er als "Lockvögel" in seinem Institut. Da er gegenüber seinen Kunden auch andere betrügerische Methoden anwandte, kam es zur Betrugsanzeige. Im Ermittlungsverfahren wurde auch sein Vorgehen im Hinblick auf die Folge bekannt. Die Staatsanwaltschaft sah daraufhin von der Verfolgung wegen eines Verstoßes gegen das BDSG (Foto als personenbezogenes Datum) gemäß § 154 StPO ab und klagte nur wegen Betrug an.

Fall 65 ("Unterstützungsunterschriften"):

Um für den Kreistag kandidieren zu können, benötigte die G-Partei eine gesetzlich bestimmte Anzahl von Unterstützungsunterschriften. Diese waren auf vorgedruckte Bögen, die zudem Name, Vorname, Geburtsdatum, Geburtsort und ersten Wohnsitz enthielten, zu leisten. Die G-Partei reichte diese Listen mit der genau erforderlichen Mindestanzahl ein. Nach Bestätigung der Richtigkeit der Wohnsitzangaben durch die Gemeinden, brachte ein Mitglied der G-Partei die Listen zum Wahlleiter. Zwei Tage später erhielt einer der Unterstützer, das Mitglied M der S-Partei (sein Bruder kandidierte für die G-Partei) ein Schreiben, indem ihm ein Parteiordnungsverfahren angedroht wurde. Daraufhin wollte M die Unterschrift zurückziehen, was er aber (zum Glück für die G-Partei) zu spät, weil nach Ablauf der Abgabefrist, versuchte. Die G-Partei schilderte diesen Sachverhalt ohne Namensnennung des M und stellte Strafantrag, da vor Ablauf der Abgabefrist (danach könne jeder die Listen einsehen) personenbezogene Daten vom Bürgermeister B an die S-Partei weitergegeben worden seien, und somit "das Datenschutzgesetz" verletzt worden sei. Nach dem Hinweis der Polizei, daß ein Strafantrag des M erforderlich sei, hielt die G-Partei mit ihm Rücksprache, M stellte aber keinen Antrag. Die Staatsanwaltschaft stellte das Verfahren daraufhin nach § 170 II StPO ein: Unabhängig davon, daß ein Strafantrag nicht vorliege, sei die Übermittlung nicht unbefugt im Sinne des Landesdatenschutzgesetzes gewesen, da es zur rechtmäßigen Aufgabenerfüllung der übermittelnden Stelle erforderlich sei. Auf "Beschwerde" der G-Partei überprüfte der Generalstaatsanwalt im Wege der Dienstaufsicht den Einstellungsbescheid und kam zum Ergebnis, daß die Übermittlung zwar nicht zuläßig sei, es aber am Strafantrag des M fehlte.

Fall 66 ("Versicherungskarteikarten":

Als im Anzeigenteil einer Zeitung "19.000 detailierte Versicherungskundenkarteikarten in denen Abschluß, Ablauf, Beitragsprämie und mehr ersichtlich" sei über eine Postfachadresse angeboten wurden, wandte sich die V-Versicherung an den Landesbeauftragten für den Datenschutz (LfD); sie vermutete, daß ihr ehemaliger Mitarbeiter M darin verwickelt sei. Der LfD gab die Angelegenheit an die Polizei ab. Diese unterrichtete ihn einige Wochen später davon, daß bisher festgestellt worden sei, daß Postfachinhaber P die Anzeige aufgegeben habe und daß in zwei Tagen seine Anzeigefrist (in diesem Bundesland besteht ein Strafantragsrecht des LfD) ablaufe. Der LfD meldete sich jedoch nicht mehr. V dagegen stellte Strafantrag "wegen Verstoßes gegen § 41 BDSG" und vermutete, daß M und P zusammenarbeiteten. Bei der Durchsuchung der Wohnungen des M und P wurden bei P 1.000 Versicherungskundenkarteikarten einer anderen Versicherung (A) und EDV-Ausdrucke der A, bei M ein Dutzend Kartons mit Abrechnungsunterlagen (einschl. Kundenkarteikarten) der V-Versicherung gefunden. Bei seiner Vernehmung gab der "selbständige Grundstücksmakler und Darlehensvermittler" P an, daß er früher bei A beschäftigt gewesen sei und diese die Unterlagen nie zurückgefordert habe. M verweigerte auf anwaltlichen Rat die Aussage vor der Polizei. Sein Anwalt schrieb daraufhin, daß die bei M gefundenen Unterlagen der V von M wegen andauernder zivilrechtlicher Auseinandersetzungen mit V zurückbehalten worden seien. Desweiteren kenne M den P überhaupt nicht.

Das Verfahren gegen M wurde abgetrennt: "Eine Verfolgung gegen den Beschuldigten M gegen Verstoßes gegen das Datenschutzgesetz kommt nicht in Betracht. Die Frage der Strafbarkeit wegen Zurückbehaltung der Karteikarten hängt von der Klärung zivilrechtlicher Fragen ab."

Bezüglich P stellte sich heraus, daß er die Versicherung A aufgefordert hatte ihre Unterlagen abzuholen, sie dies jedoch nicht getan hatte. Danach wurde das Verfahren gegen P gemäß § 170 II StPO eingestellt: "Soweit ein Verstoß gegen § 41 des Bundesdatenschutzgesetzes (BDSG) in Betracht kam, kann dem Beschuldigten P in keinem Fall die Weitergabe von geschützten Daten nachgewiesen werden. Die Zeitungsanzeige, in der er Versicherungsunterlagen zum Verkauf angeboten hat, deutet zwar auf ein entsprechendes Vorhaben hin, es konnte jedoch nur ein einziger Interessent ermittelt werden und auch mit diesem ist es nicht zum Abschluß eines Vertrages und insbesondere nicht zur Übergabe von Versicherungsunterlagen gekommen. Der Versuch ist nicht strafbar." Auch eine Unterschlagung sei ihm nicht nachzuweisen.

Fall 67("Programmdopplung"):

Der Programmierer P war vom Inkasskounternehmen I mit der Erstellung eines Programmes beauftragt gewesen. Nachdem er es fertiggestellt hatte, kopierte er dies, sowie weitere (u.a. auch eines mit Schuldneradressen) an einem Samstag auf einen mitgebrachten Magnetplattenturm und nahm darüberhinaus von I entwickelte Druckformulare sowie Schuldnerlisten mit. Später verkaufte er die Programme an verschiedene Firmen. Als I dies erfuhr, erstattete es Anzeige (wegen §§ 7, 18 UWG, 106, 109 UrhG, 242, 246, 266, 248a StGB) und stellte die erforderlichen Strafanträge.

Nach umfangreichen Ermittlungen, in die auch EDV-Spezialisten des LKA eingeschaltet waren, wurde knapp zwei Jahre nach Anzeigeneingang das Verfahren gemäß § 154 d StGB eingestellt, da der Ausgang des inzwischen zur Frage, wem die Computerprogramme gehören, anstrengten zivilrechtlichen Verfahrens, abgewartet werden sollte. Am 9.2.1983 wurde vom OLG Karlsruhe das Berufungsurteil verkündet (vgl. BB 1983, 986 ff.). Nachdemdie Revision beim BHG anhängig gemacht worden war, beantragte die Staatsanwaltschaft wegen drohender Verjährung im Februar 1984 den Erlaß eines Strafbefehls gegen P, u.a. weil er unbefugt personenbezogene Daten "übermittelt oder abgerufen" habe. Vorgeworfen wurden P Verstöße gegen § 106 UrhG, §§ 17 II, 18 UWG, § 41 I Ziff. 1 und 2 BDSG, §§ 246, 248 a StGB. Unter den über hundert als Beweismittel angegebenen Urkunden befanden sich auch Computerausdrucke "zum Nachweis unbefugter Übertragung von Schuldneradressen. Gegen den vom Schöffengericht erlassenen Strafbefehl in Höhe von 300 Tagessätzen legte P Einspruch ein.

1) Sieber bezeichnet diesen Fall in seinem Buch (Computerkriminalität und Strafrecht) als "Programmdopplungs-Fall", weshalb auch hier dieser Name verwendet wird.

Fall 68 ("Handwerkersorgen"):

Der vermögende Handwerksmeister H ist besorgt über den Umgang seiner einzigen und schon älteren Tochter T mit dem wesentlich älteren und mehrfach geschiedenen Assistenten A und versucht deshalb über verschiedene Quellen näheres über A zu erfahren. Er beauftragt die Detektive D, die einen Bericht etstellen und über einen Dritten erlangt er eine Auskunft einer Auskunftei. A erfährt dies über T, die ihm auch aus den Berichten des D vorliest. Er erstattet Strafanzeige wegen Beleidigung und stellt Strafantrag gegen Unbekannt, zudem erhebt er schließlich eine zivilrechtliche Unterlassungsklage. Aufgrund von Zeugenaussagen stellt sich heraus, daß keine beleidigenden Äußerungen weitergetragen wurden, die Ermittlungen ergeben jedoch, daß - wie es in einem Vermerk steht - der Beschuldigte H "unter Zuhilfenahme des Zeugen Z in mittelbarer Täterschaft eine Auskunft der Auskunftei einholen habe lassen über den A, ohne hierzu befugt gewesen zu sein." Er habe deshalb nicht offenkundige Daten "nach § 41 BDSG in Verbindung mit § 21 NDSG abgerufen."

Die Staatsanwaltschaft teilte dem H darauf mit, daß sie beabsichtige, das Verfahren "wegen Verstoßes gegen das Datenschutzgesetz" nach § 153 a StPO gegen eine Zahlung von 500,-- DM einzustellen. Der Rechtsanwalt des H schrieb hierauf, daß der nach § 41 III BDSG erforderliche Strafantrag verspätet gestellt sei (was objektiv zutrifft). Bezüglich § 21 III NDSG habe er im Hinblick auf Art. 31 GG Zweifel an dessen Verfassungsmäßigkeit. Ferner sei das öffentliche Interesse bei diesem "Familienkrieg" nicht gegeben und außerdem liege kein Abrufen im Sinne des § 41 I Ziff. 2 BDSG vor. Als dann zwischen H und A ein außergerichtlicher Vergleich geschlossen worden war, zog A seinen Strafantrag zurück. Darauf wurde das Verfahren mit Zustimmung des Gerichts gemäß § 153 I StPO eingestellt: Zwar habe sich H "des Verdachtes eines Vergehens gegen das Datenschutzgesetz ausgesetze", da es sich aber um private Streitigkeiten familiärer Art handele und der Geschädigte kein Interesse an der Strafverfolgung habe, bestehe lediglich der Verdacht eines geringen Verschuldens.

Fall 69 ("Scheidungsfolgen"):

Der geschiedene Ehemann und Kaufmann K hatte eine Handelsauskunftei über das Vorliegen eines berechtigten Interesses (§ 32 II BDSG) getäuscht und deshalb personenbezogene Daten über den Anzeigenerstatter A, der mit K's geschiedener Frau zusammenlebte, erhalten. Die Daten, die das wirtschaftliche Verhältnis des A betrafen, gab K an das Sozialamt weiter. Die Staatsanwaltschaft stellte das Verfahren gegen den beschuldigten K mit folgender Begründung gemäß § 170 II StPO ein:

"Vorliegend wurden von der Auskunftei personenbezogene Daten an den Beschuldigten als Dritten übermittelt. Weil er diese Daten nicht in einer Datei gespeichert hat, stellt sein Weitergeben an das Sozialamt kein Übermitteln im Sinne des Gesetzes dar. Die Daten waren bei dem Beschuldigten frei verfügbar (vgl. Ordemann/Schomerus, BDSG, 2. Aufl. § 2 Anm. 2.2)."

Das Verfahren gegen die Auskunftei wegen unbefugter Datenübermittlung wurde eingestellt. Sie habe aufgrund der Geschäftsbeziehungen zwischen ihr und K davon ausgehen können, daß seine Angaben richtig waren.

Fall StA Berlin:

Ende 1980 hatte die "Notgemeinschaft für eine freie Universität" in Berlin zum wiederholten Male eine Liste von im wesentlichen an der FU in Berlin tätigen Wissenschaftlern veröffentlicht und die Genannten politisch linker Tendenzen verdächtigt. Das Verfahren wurde eingestellt, die dagegen erhobene Beschwerde blieb erfolglos. Die Staatsanwaltschaft lehnte es ab, den Dateibegriff dahingehend auszulegen, daß auch das Umarbeiten einer nach bestimmten Gesichtspunkten geordneten Liste durch Umsortieren und Ergänzen mit dem Ergebnis der Erstellung einer neuen, geordneten Liste als Datenverarbeitungsvorgang unter Verwendung einer Datei gewertet werden könne. Ferner bejahte sie die Anwendung des Medienprivilegs für den geschilderten Fall der Veröffentlichung von Daten in Form einer Broschüre.

AUSWERTUNGSBOGEN

Lfd. Nr. (Eingangs-Nr.):

StA ...../ Js / 19 /Land:

Beginn: 19

Ende: 19 / Dauer: Monate

VERFAHRENSEINLEITUNG:

WIE wurde Verfahren eingeleitet? (Anzeige/von Amts wegen):

WO wurde Anzeige angebracht?

Bei Polizei-O StA-O LfD/BfD-O sonst.:

VON WEM wurde Anzeige angebracht?

Vom Betroff. selbst-O seinem RA-O LfD/BfD-O sonst.:

LfD/BfD und/oder Aufsichtsbehörde eingeschaltet?

Was war der Grund der Anzeige? Verstoß gg Datenschutz-O

Diebstahl-O Amtsdelikte-O sonst.:

STRAFANTRAG:

Wurde Strafantrag gestellt? Ja, sofort-O Ja, später-O

Ja, zu spät-O zurückgezogen-O NEIN-O weil nicht gewußt-O

VON WEM wurde Antrag gestellt?

Vom Betroff.-O LfD-O speich. Stelle-O

Wie beurteilte dies StA? (Niedersachsen: Behandlung des öffentl. Interesses!):

DATEN:

Welche Art von Daten? (genaue Bezeichnung/Charakterisierung!):

- Personenbezogen: Nach StA: Ja-O Nein-O Nach h. L.: Ja-O Nein-O
- Offenkundig: Nach StA: Ja-O Nein-O Nach h. L.: Ja-O Nein-O

Wo befanden sich die Daten?

EDV-Anlage-O Graubereich-O Nicht-Datei-O Unbekannt-O

Genaue Art/Bezeichnung des Speicherorts und Eigentümers:

TATMODALITÄTEN:

Was wurde Beschuldigten vorgeworfen?

Wie wurden die Tatmodalitäten von StA gesehen/beurteilt?

übermitteln: Zirkel bzw. Def. gesehen? Besonderheiten? Synonyme?

verändern: Def.? verknüpfen?

speichern: Def.?

löschen: Def. ?

abrufen: technisch?

sich verschaffen: Diebstahl oder nur beschaffen?

Besonderheiten insgesamt?

Bereich/Sphäre des Verstoßes:

- Öff. Bereich: Bund-O Land-O Gemeinde-O Anstalt etc.
- Priv. Bereich: Privatperson -O Unternehmen mit eig. DV-O
  AuftragsDV-O Auskunftei-O sonst.:

WELCHES GESETZ einschlägig:

StA:	BDSG-O	LDSG-O	beide/offen-O
Lit.:	BDSG-O	LDSG-O	nicht klärbar-O

Besonderheiten (SGB X!):

TÄTER/BESCHULDIGTER:

Wer wurde vom Anzeigenerstatter beschuldigt?

Anzahl der als beschuldigt vernommenen Personen:
Fam.-stand: led.-O verh.-O unbekannt-O sonst.:
männl.-O weibl.-O Alter: J. Kinder:
Nationalität: D-O sonst.:
Beruf: Arbeitgeber: Privat-O Staat-O
Wegen anderer Delikte vorbestraft?
Nein-O Ja-O, wegen: Unbekannt-O
Gewaltanwendung?
Von wem Daten erhalten: Selbst besorgt-O gutgl. Dritter-O bösgl. Dr.-O
vom Opfer selbst aufgrund .....

Verteidiger: Ja-O Nein-O
Erste Vernehmung: Vor Pol.-O StA-O Richter-O
Schriftl. Vernehmung-O
Reaktion des Beschuldigten: Geständig-O Aussageverweigerung-O
sonst. bzw. Einlassungen:

Zweite Vernehmung:

Was war Grund (Tatmotiv) des Handelns?
unbekannt-O kommerziell/geschäftl.-O privat/persönl.-O
dienstl./behörd.-O sonstig:

WELCHE Beschuldigten - Opfer - Beziehung? direkter Kontakt-O
verwandt-O befreundet-O benachbart-O dienstl./behördl.-O
geschäftl./berufl.-O und in gl. Firma-O gl. Behörde-O
KEINERLEI-O sonstig:

WER war Opfer/Geschädigter (Art und Anzahl):

Entstand ein Schaden?

TATORT:

über 500 000 Einw.-O 100-500-Ts.-O unter 100 000 Einw.-O

AUFKLÄRUNG des Sachverhalts?

"Beweismittel", insbesondere Sachverständige:

Richter nötig? Hausdurchsuchung?

Verzögerung der Aufklärung ("Mauern")?

VERFAHRENSBEENDIGUNG:

Erste verfahrensbeendende Handlung der StA:

- Einstellung nach 152 II StPO-O 170 II-O
  Begründung bei 152/170 (pro Beschuld. + Mehrfachnennung):

- nach 153-O 153 a-O in Höhe von:

Antrag auf Erlaß Strafbefehl-O (Grund/Höhe)

Antrag auf Eröffnung HV-O

FORTGANG des Verfahrens (u. a. Beschwerde?/Verurteilung ?):

L e b e n s l a u f

Am 14. März 1957 wurde ich in Göppingen als erster von drei Söhnen des Notars Martin Herb und seiner Ehefrau Gertrud geb. Wieler geboren. In Lorch im Remstal wuchs ich auf und ging in die dortige Volksschule.

Nach dem Umzug meiner Eltern nach Stuttgart besuchte ich dort das Wagenburg-Gymnasium, an welchem ich am 19.5.1976 das Abitur ablegte.

Mit dem Wintersemester 1976/77 begann ich das Studium der Rechtswissenschaften an der Eberhard-Karls-Universität zu Tübingen. Nach dem vierten Semester wechselte ich für zwei Semester an die Universitäten Genf und Lausanne. Die Erste juristische Staatsprüfung legte ich am 18.6.1982 in Tübingen ab.

Am 1.9.1982 begann ich meine Referendarausbildung beim Landgericht Stuttgart, die bis zum heutigen Tage andauert.

Vom 1.10.1982 bis 31.12.1983 war ich daneben als wissenschaftliche Hilfskraft am Lehrstuhl von Prof.Dr. F. Haft an der Universität Tübingen tätig.

dissertationsdruck · vervielfältigungen
f. u. t. müllerbader
Forststraße 18 · 7024 Filderstadt 4 (Plattenhardt)
Telefon (07 11) 77 15 67